

EXHIBIT 1

Well, These New Zuckerberg IMs Won't Help Facebook's Privacy Problems

Nicholas Carlson



<http://www.flickr.com/photos/prospere/2927938192/sizes/l/>>Ludovic Toinel

Facebook CEO Mark Zuckerberg and his company are suddenly facing a big new round of scrutiny and criticism about their cavalier attitude toward user privacy.

An early instant messenger exchange Mark had with a college friend won't help put these concerns to rest.

According to SAI sources, the following exchange is between a 19-year-old Mark Zuckerberg and a friend shortly after Mark launched The Facebook in his dorm room:

Zuck: Yeah so if you ever need info about anyone at Harvard

Zuck: Just ask.

Zuck: I have over 4,000 emails, pictures, addresses, SNS

[Redacted Friend's Name]: What? How'd you manage that one?

Zuck: People just submitted it.

Zuck: I don't know why.

Zuck: They "trust me"

Zuck: Dumb fucks.

Brutal.

Could Mark have been completely joking? Sure. But the exchange does reveal that [Facebook's aggressive attitude toward privacy](#) may have begun early on.

Since Facebook launched, the company has faced one privacy flap after another, usually following changes to the privacy policy or new product releases. To its credit, the company has often modified its products based on such feedback. As the pioneer in a huge new market, Facebook will take heat for everything it does. It has also now grown into a \$22 billion company run by adults who know that [their future depends on Facebook users trusting the site's privacy policy](#).

But the company's attitude toward privacy, as reflected in [Mark's early emails and IMs](#), features like Beacon and Instant Personalization, and the frequent changes to the privacy policy, has been consistently aggressive: Do something first, then see how people react.

And this does appear to reflect Mark's own views of privacy, which seem to be that people shouldn't care about it as much as they do -- an attitude that very much reflects the attitude of his generation.

After all, here's what early Facebook engineering boss, Harvard alum, and Zuckerberg confidant Charlie Cheever said in David Kirkpatrick's brilliantly-reported upcoming book [The Facebook Effect](#).

"I feel Mark doesn't believe in privacy that much, or at least believes in privacy as a stepping stone. Maybe he's right, maybe he's wrong."

Again in Kirkpatrick's book, Facebook COO Sheryl Sandberg puts it this way:

"Mark really does believe very much in transparency and the vision of an open society and open world, and so he wants to push people that way. I think he also understands that the way to get there is to give people granular control and comfort. He hopes you'll get more open, and he's kind of happy to help you get there. So for him, it's more of a means to an end. For me, I'm not as sure."

Facebook declined to comment about Mark's attitude toward privacy.

Update: [Facebook Issues Statement On Latest Zuckerberg IM And Company Attitude Toward Privacy](#)

See also:

[How To Put Facebook On A Privacy Lockdown](#)

[At Last -- The Full Story Of How Facebook Was Founded](#)

EXHIBIT 2

Facebook Gave Device Makers Deep Access to Data on Users and Friends

The company formed data-sharing partnerships with Apple, Samsung and dozens of other device makers, raising new concerns about its privacy protections.

By GABRIEL J.X. DANCE, NICHOLAS CONFESSORE and MICHAEL LaFORGIA JUNE 3, 2018

As Facebook sought to become the world's dominant social media service, it struck agreements allowing phone and other device makers access to vast amounts of its users' personal information.

Facebook has reached data-sharing partnerships with at least 60 device makers — including Apple, Amazon, BlackBerry, Microsoft and Samsung — over the last decade, starting before Facebook apps were widely available on smartphones, company officials said. The deals allowed Facebook to expand its reach and let device makers offer customers popular features of the social network, such as messaging, “like” buttons and address books.

But the partnerships, whose scope has not previously been reported, raise concerns about the company's privacy protections and compliance with a 2011 consent decree with the Federal Trade Commission. Facebook allowed the device companies access to the data of users' friends without their explicit consent, even after declaring that it would no longer share such information with outsiders. Some device makers could retrieve personal information even from users' friends who believed they had barred any sharing, The New York Times found.

[Here's what we know about Facebook's partnerships with device makers.]

Most of the partnerships remain in effect, though Facebook began winding them down in April. The company came under intensifying scrutiny by lawmakers and regulators after news reports in March that a political

consulting firm, Cambridge Analytica, misused the private information of tens of millions of Facebook users.

In the furor that followed, Facebook's leaders said that the kind of access exploited by Cambridge in 2014 was cut off by the next year, when Facebook prohibited developers from collecting information from users' friends. But the company officials did not disclose that Facebook had exempted the makers of cellphones, tablets and other hardware from such restrictions.

"You might think that Facebook or the device manufacturer is trustworthy," said Serge Egelman, a privacy researcher at the University of California, Berkeley, who studies the security of mobile apps. "But the problem is that as more and more data is collected on the device — and if it can be accessed by apps on the device — it creates serious privacy and security risks."

In interviews, Facebook officials defended the data sharing as consistent with its privacy policies, the F.T.C. agreement and pledges to users. They said its partnerships were governed by contracts that strictly limited use of the data, including any stored on partners' servers. The officials added that they knew of no cases where the information had been misused.

The company views its device partners as extensions of Facebook, serving its more than two billion users, the officials said.

"These partnerships work very differently from the way in which app developers use our platform," said Ime Archibong, a Facebook vice president. Unlike developers that provide games and services to Facebook users, the device partners can use Facebook data only to provide versions of "the Facebook experience," the officials said.

Some device partners can retrieve Facebook users' relationship status, religion, political leaning and upcoming events, among other data. Tests by The Times showed that the partners requested and received data in the same way other third parties did.

Facebook's view that the device makers are not outsiders lets the partners go even further, The Times found: They can obtain data about a user's

Facebook friends, even those who have denied Facebook permission to share information with any third parties.

In interviews, several former Facebook software engineers and security experts said they were surprised at the ability to override sharing restrictions.

“It’s like having door locks installed, only to find out that the locksmith also gave keys to all of his friends so they can come in and rifle through your stuff without having to ask you for permission,” said Ashkan Soltani, a research and privacy consultant who formerly served as the F.T.C.’s chief technologist.

Details of Facebook’s partnerships have emerged amid a reckoning in Silicon Valley over the volume of personal information collected on the internet and monetized by the tech industry. The pervasive collection of data, while largely unregulated in the United States, has come under growing criticism from elected officials at home and overseas and provoked concern among consumers about how freely their information is shared.

In a tense appearance before Congress in March, Facebook’s chief executive, Mark Zuckerberg, emphasized what he said was a company priority for Facebook users. “Every piece of content that you share on Facebook you own,” he testified. “You have complete control over who sees it and how you share it.”

But the device partnerships provoked discussion even within Facebook as early as 2012, according to Sandy Parakilas, who at the time led third-party advertising and privacy compliance for Facebook’s platform.

“This was flagged internally as a privacy issue,” said Mr. Parakilas, who left Facebook that year and has recently emerged as a harsh critic of the company. “It is shocking that this practice may still continue six years later, and it appears to contradict Facebook’s testimony to Congress that all friend permissions were disabled.”

The partnerships were briefly mentioned in documents submitted to German lawmakers investigating the social media giant’s privacy practices

and released by Facebook in mid-May. But Facebook provided the lawmakers with the name of only one partner — BlackBerry, maker of the once-ubiquitous mobile device — and little information about how the agreements worked.

The submission followed testimony by Joel Kaplan, Facebook's vice president for global public policy, during a closed-door German parliamentary hearing in April. Elisabeth Winkelmeier-Becker, one of the lawmakers who questioned Mr. Kaplan, said in an interview that she believed the data partnerships disclosed by Facebook violated users' privacy rights.

“What we have been trying to determine is whether Facebook has knowingly handed over user data elsewhere without explicit consent,” Ms. Winkelmeier-Becker said. “I would never have imagined that this might even be happening secretly via deals with device makers. BlackBerry users seem to have been turned into data dealers, unknowingly and unwillingly.”

In interviews with The Times, Facebook identified other partners: Apple and Samsung, the world's two biggest smartphone makers, and Amazon, which sells tablets.

An Apple spokesman said the company relied on private access to Facebook data for features that enabled users to post photos to the social network without opening the Facebook app, among other things. Apple said its phones no longer had such access to Facebook as of last September.

Samsung declined to respond to questions about whether it had any data-sharing partnerships with Facebook. Amazon also declined to respond to questions.

Usher Lieberman, a BlackBerry spokesman, said in a statement that the company used Facebook data only to give its own customers access to their Facebook networks and messages. Mr. Lieberman said that the company “did not collect or mine the Facebook data of our customers,” adding that “BlackBerry has always been in the business of protecting, not monetizing, customer data.”

Microsoft entered a partnership with Facebook in 2008 that allowed Microsoft-powered devices to do things like add contacts and friends and receive notifications, according to a spokesman. He added that the data was stored locally on the phone and was not synced to Microsoft's servers.

Facebook acknowledged that some partners did store users' data — including friends' data — on their own servers. A Facebook official said that regardless of where the data was kept, it was governed by strict agreements between the companies.

"I am dumbfounded by the attitude that anybody in Facebook's corporate office would think allowing third parties access to data would be a good idea," said Henning Schulzrinne, a computer science professor at Columbia University who specializes in network security and mobile systems.

The Cambridge Analytica scandal revealed how loosely Facebook had policed the bustling ecosystem of developers building apps on its platform. They ranged from well-known players like Zynga, the maker of the FarmVille game, to smaller ones, like a Cambridge contractor who used a quiz taken by about 300,000 Facebook users to gain access to the profiles of as many as 87 million of their friends.

Those developers relied on Facebook's public data channels, known as application programming interfaces, or APIs. But starting in 2007, the company also established private data channels for device manufacturers.

At the time, mobile phones were less powerful, and relatively few of them could run stand-alone Facebook apps like those now common on smartphones. The company continued to build new private APIs for device makers through 2014, spreading user data through tens of millions of mobile devices, game consoles, televisions and other systems outside Facebook's direct control.

Facebook began moving to wind down the partnerships in April, after assessing its privacy and data practices in the wake of the Cambridge Analytica scandal. Mr. Archibong said the company had concluded that the partnerships were no longer needed to serve Facebook users. About 22 of them have been shut down.

The broad access Facebook provided to device makers raises questions about its compliance with a 2011 consent decree with the F.T.C.

The decree barred Facebook from overriding users' privacy settings without first getting explicit consent. That agreement stemmed from an investigation that found Facebook had allowed app developers and other third parties to collect personal details about users' friends, even when those friends had asked that their information remain private.

After the Cambridge Analytica revelations, the F.T.C. began an investigation into whether Facebook's continued sharing of data after 2011 violated the decree, potentially exposing the company to fines.

Facebook officials said the private data channels did not violate the decree because the company viewed its hardware partners as "service providers," akin to a cloud computing service paid to store Facebook data or a company contracted to process credit card transactions. According to the consent decree, Facebook does not need to seek additional permission to share friend data with service providers.

"These contracts and partnerships are entirely consistent with Facebook's F.T.C. consent decree," Mr. Archibong, the Facebook official, said.

But Jessica Rich, a former F.T.C. official who helped lead the commission's earlier Facebook investigation, disagreed with that assessment.

"Under Facebook's interpretation, the exception swallows the rule," said Ms. Rich, now with the Consumers Union. "They could argue that any sharing of data with third parties is part of the Facebook experience. And this is not at all how the public interpreted their 2014 announcement that they would limit third-party app access to friend data."

To test one partner's access to Facebook's private data channels, The Times used a reporter's Facebook account — with about 550 friends — and a 2013 BlackBerry device, monitoring what data the device requested and received. (More recent BlackBerry devices, which run Google's Android operating system, do not use the same private channels, BlackBerry officials said.)

Immediately after the reporter connected the device to his Facebook account, it requested some of his profile data, including user ID, name, picture, “about” information, location, email and cellphone number. The device then retrieved the reporter’s private messages and the responses to them, along with the name and user ID of each person with whom he was communicating.

The data flowed to a BlackBerry app known as the Hub, which was designed to let BlackBerry users view all of their messages and social media accounts in one place.

The Hub also requested — and received — data that Facebook’s policy appears to prohibit. Since 2015, Facebook has said that apps can request only the names of friends using the same app. But the BlackBerry app had access to all of the reporter’s Facebook friends and, for most of them, returned information such as user ID, birthday, work and education history and whether they were currently online.

The BlackBerry device was also able to retrieve identifying information for nearly 295,000 Facebook users. Most of them were second-degree Facebook friends of the reporter, or friends of friends.

In all, Facebook empowers BlackBerry devices to access more than 50 types of information about users and their friends, The Times found.

Katrin Bennhold contributed reporting.

Related Coverage

- [Facebook’s Device Partnerships Explained](#)
JUNE 4, 2018
 - [Facebook Says Cambridge Analytica Harvested Data of Up to 87 Million Users](#) APRIL 4, 2018
 - [Facebook Faces Growing Pressure Over Data and Privacy Inquiries](#) MARCH 20, 2018
- [How Trump Consultants Exploited the](#)

Facebook Data of Millions

MARCH 17, 2018

© 2021 The New York Times Company

The New York Times
<https://nyti.ms/2Hh5sbn>

EXHIBIT 3

The New York Times | <https://www.nytimes.com/2019/05/09/opinion/sunday/chris-hughes-facebook-zuckerberg.html>

Opinion

It's Time to Break Up Facebook

By Chris Hughes

May 9, 2019

The last time I saw Mark Zuckerberg was in the summer of 2017, several months before the Cambridge Analytica scandal broke. We met at Facebook's Menlo Park, Calif., office and drove to his house, in a quiet, leafy neighborhood. We spent an hour or two together while his toddler daughter cruised around. We talked politics mostly, a little about Facebook, a bit about our families. When the shadows grew long, I had to head out. I hugged his wife, Priscilla, and said goodbye to Mark.

Since then, Mark's personal reputation and the reputation of Facebook have taken a nose-dive. The company's mistakes — the sloppy privacy practices that dropped tens of millions of users' data into a political consulting firm's lap; the slow response to Russian agents, violent rhetoric and fake news; and the unbounded drive to capture ever more of our time and attention — dominate the headlines. **It's been 15 years since I co-founded Facebook at Harvard**, and I haven't worked at the company in a decade. But I feel a sense of anger and responsibility.

Watch: A founder of Facebook says it should be broken up.

Mark is still the same person I watched hug his parents as they left our dorm's common room at the beginning of our sophomore year. He is the same person who procrastinated studying for tests, fell in love with his future wife while in line for the bathroom at a party and slept on a mattress on the floor in a small apartment years after he could have afforded much more. In other words, he's human. But it's his very humanity that makes his unchecked power so problematic.

Mark's influence is staggering, far beyond that of anyone else in the private sector or in government. He controls three core communications platforms — Facebook, Instagram and WhatsApp — that billions of people use every day. Facebook's board works more like an advisory committee than an overseer, because Mark controls around 60 percent of voting shares. Mark alone can decide how to configure Facebook's algorithms to determine what people see in their News Feeds, what privacy settings they can use and even which messages get delivered. He sets the rules for how to distinguish violent and incendiary speech from the merely offensive, and he can choose to shut down a competitor by acquiring, blocking or copying it.

Mark is a good, kind person. But I'm angry that his focus on growth led him to sacrifice security and civility for clicks. I'm disappointed in myself and the early Facebook team for not thinking more about how the News Feed algorithm could change our culture, influence elections and empower nationalist leaders. And I'm worried that Mark has surrounded himself with a team that reinforces his beliefs instead of challenging them.

The government must hold Mark accountable. For too long, lawmakers have marveled at Facebook's explosive growth and overlooked their responsibility to ensure that Americans are protected and markets are competitive. Any day now, the Federal Trade Commission is expected to impose a \$5 billion fine on the company, but that is not enough; nor is Facebook's offer to appoint some kind of privacy czar. After Mark's congressional testimony last year, there should have been calls for him to truly reckon with his mistakes. Instead the legislators who questioned him were derided as too old and out of touch to understand how tech works. That's the impression Mark wanted Americans

‘Don’t be too proud to copy.’”

(There is little regulators can do about this tactic: Snapchat patented its “ephemeral message galleries,” but copyright law does not extend to the abstract concept itself.)

Would-be competitors can’t raise the money to take on Facebook.

As a result of all this, would-be competitors can’t raise the money to take on Facebook. Investors realize that if a company gets traction, Facebook will copy its innovations, shut it down or acquire it for a relatively modest sum. So despite an extended economic expansion, increasing interest in high-tech start-ups, an explosion of venture capital and growing public distaste for Facebook, no major social networking company has been founded since the fall of 2011.

As markets become more concentrated, the number of new start-up businesses declines. This holds true in other high-tech areas dominated by single companies, like search (controlled by Google) and e-commerce (taken over by Amazon). Meanwhile, there has been plenty of innovation in areas where there is no monopolistic domination, such as in workplace productivity (Slack, Trello, Asana), urban transportation (Lyft, Uber, Lime, Bird) and cryptocurrency exchanges (Ripple, Coinbase, Circle).

I don’t blame Mark for his quest for domination. He has demonstrated nothing more nefarious than the virtuous hustle of a talented entrepreneur. Yet he has created a leviathan that crowds out entrepreneurship and restricts consumer choice. It’s on our government to ensure that we never lose the magic of the invisible hand. How did we allow this to happen?

Since the 1970s, courts have become increasingly hesitant to break up companies or block mergers unless consumers are paying inflated prices that would be lower in a competitive market. But a narrow reliance on whether or not consumers have experienced price gouging fails to take into account the full cost of market domination. It doesn’t recognize that we also want markets to be competitive to encourage innovation and to hold power in check. And it is out of step with the history of antitrust law. Two of the last major antitrust suits, against AT&T and IBM in the 1980s, were grounded in the argument that they had used their size to stifle innovation and crush competition.

As the Columbia law professor Tim Wu writes, “It is a disservice to the laws and their intent to retain such a laserlike focus on price effects as the measure of all that antitrust was meant to do.”

Facebook is the perfect case on which to reverse course, precisely because Facebook makes its money from targeted advertising, meaning users do not pay to use the service. But it is not actually free, and it certainly isn’t harmless.

We pay for Facebook with our data and our attention, and by either measure it doesn’t come cheap.

Facebook’s business model is built on capturing as much of our attention as possible to encourage people to create and share more information about who they are and who they want to be. **We pay for Facebook with our data and our attention, and by either measure it doesn’t come cheap.**

I was on the original News Feed team (my name is on the patent), and that product now gets billions of hours of attention and pulls in unknowable amounts of data each year. The average Facebook user spends an hour a day on the platform; Instagram users spend 53 minutes a day scrolling through pictures and videos. They create immense amounts of data — not just likes and dislikes, but how many seconds they watch a particular video — that Facebook uses to refine its targeted advertising. Facebook also collects data from partner companies and apps, without most users knowing about it, according to testing by The Wall Street Journal.

Some days, lying on the floor next to my 1-year-old son as he plays with his dinosaurs, I catch myself scrolling through Instagram, waiting to see if the next image will be more beautiful than the last. What am I doing? I know it’s not good for me, or for my son, and yet I do it anyway.

The choice is mine, but it doesn’t feel like a choice. Facebook seeps into every corner of our lives to capture as much of our attention and data as possible and, without any alternative, we make the trade.

EXHIBIT 4

Facebook Executive Discusses Beacon Brouhaha

Brad Stone

Update: *The interview below took place hours before Facebook announced a major change in its Beacon system, one that requires users to explicitly approve the sending of information to their friends' News Feeds. See [our article](#) for details.*

Facebook does not appear to be conceding much ground on Beacon — the program that informs a person's Facebook friends what he has purchased or posted on sites like Fandango.com, Yelp.com and NYTimes.com.

Earlier today I spoke with Chamath Palihapitiya, vice president of product marketing and operations at Facebook. Mr. Palihapitiya said the company was listening to its users and described three changes Facebook was making to Beacon. First, the opt-out boxes on Beacon partner sites, which let users specify if they do not want their Facebook friends to be notified of their purchases or online activity, will now load more quickly, ensuring that more users see them.

Second, Facebook will now be able to determine whether the opt-out notification has been properly loaded on the user's screen — an indication of whether the user has actually been given an opportunity to opt-out.

Finally, if users fail to approve or decline the Facebook alert on the partner site, Facebook will no longer assume the user is agreeing by omission. Instead, it will offer another, more visible opportunity to opt-out to users on Facebook itself. If no action is taken within two days, Facebook will assume the user complies and will publish the action in the news feed.

"We don't want to catch anyone off guard," Mr. Palihapitiya said. "We are giving them an explicit and clear way to know what has happened and for them to publish."

More information on Beacon from our conversation:

Q. Will Facebook ever make Beacon "opt-in" instead of "opt-out," as critics have suggested, or simply give users a single way to decline to participate in the service altogether?

A. Mr. Palihapitiya said the company learned from the similar controversy over the introduction of the News Feed last year that people need to be given a chance to try new features. "We think Beacon has the same potential" as News Feed, he said. "We want people to try it, to see it in action. If they don't like it they can easily turn it off. Our point of view is, let's give people the ability to sample it."

Q. Why not give people a universal opt-out of the Beacon service?

A. "We think the right way to offer this is on a site-by-site basis. We want people to

see how the product behaves on different sites.”

Q. But some people are asking for a single opt-out.

A. “One of the things we try to do is listen to feedback as much as possible. Just to give you where a lot of this feedback is coming from, it’s coming more from the press than specific users,” he said. “Right now, the right thing to do is to make sure we speak to actual users, not the pundits.”

Q. It’s not pundits though — it is users and advocates concerned about privacy.

A. “I’m not trying to diminish that,” he said. “The feedback we’ve gotten from actual users using this product has allowed us to refine it, and here’s the first set of changes. If there is demand for a different set of features, we’ll do that as well.”

Q. If I buy tickets on Fandango, and decline to publish the purchase to my friends on Facebook, does Facebook still receive the information about my purchase?

A. “Absolutely not. One of the things we are still trying to do is dispel a lot of misinformation that is being propagated unnecessarily.”

Q. Were users properly informed about Beacon from the start?

A. “The way that we announce products is generally through blogging and through Rooster stories,” he said, referring to prominent alerts from Facebook that appear in users’ News Feeds. “We followed that exact same protocol for this product that we followed for many other product releases in the past. What we don’t do is proactively push e-mail or other things to users. What we try to do is use the service itself to communicate about improvements and features we make. But our takeaway is we need to make sure we do a better and better job on that.”

Q. I think MoveOn will see this as you guys digging in.

A. “The thing is, we haven’t dug in in any way. We have pretty markedly changed the product based on the feedback we’ve gotten. What I’m saying is, it’s still important that people have a chance to see it and make a decision for themselves.”

EXHIBIT 5

'Like' Button Follows Web Users

Amir Efrati

Internet users tap Facebook Inc.'s "Like" and Twitter Inc.'s "Tweet" buttons to share content with friends. But these tools also let their makers collect data about the websites people are visiting.

These so-called social widgets, which appear atop stories on news sites or alongside products on retail sites, notify Facebook and Twitter that a person visited those sites even when users don't click on the buttons, according to a study done for The Wall Street Journal.

These widgets are prolific. They have been added to millions of web pages in the past year. Facebook's buttons appear on a third of the world's 1,000 most-visited websites, according to the study. Buttons from Twitter and Google appear on 20% and 25% of those sites, respectively.

The widgets, which were created to make it easy to share content with friends and to help websites attract visitors, are a potentially powerful way to track Internet users. They could link users' browsing habits to their social-networking profile, which often contains their name.

For example, Facebook or Twitter know when one of their members reads an article about filing for bankruptcy on MSNBC.com or goes to a blog about depression called Fighting the Darkness, even if the user doesn't click the "Like" or "Tweet" buttons on those sites.

For this to work, a person only needs to have logged into Facebook or Twitter once in the past month. The sites will continue to collect browsing data, even if the person closes their browser or turns off their computers, until that person explicitly logs out of their Facebook or Twitter accounts, the study found.

Facebook, Twitter, Google and other widget-makers say they don't use browsing data generated by the widgets to track users; Facebook says it only uses the data for advertising purposes when a user clicks on a widget to share content with friends.

Facebook and Google, which has a widget for its "Buzz" social-networking service, say they "anonymize" browsing data so the information is not traced to a particular user. Facebook says the data are deleted within 90 days, while Google says data are deleted within two weeks. Facebook and Google say they use the information to measure the widgets' effectiveness and help other websites attract visitors.

Twitter says it doesn't use such browsing data and deletes it "quickly." A spokesman says the company could in theory use the data to "surface better content" for users in the future.

Revelations about the social widgets come amid growing concern about the privacy of Internet and smartphone users. Members of Congress have introduced at least five privacy-related bills this year, including three that aim to create a mechanism that would let users disable tracking.

Some privacy advocates express concerns, citing prior Facebook and Google stumbles over privacy issues.

"Our reading habits online encompass everything we're thinking about, political and religious views, health and relationship problems," said Peter Eckersley, a senior technologist at the

Electronic Frontier Foundation, a privacy-advocacy group. "Do you want to have an invisible person peering over your shoulder as you walk through the library?"

Advertisement - Scroll to Continue

Widget makers say the collection of users' Web-browsing activity is an unintended side effect of how the tools work. In order to show a user which of their online friends "liked" a particular article, for example, the widget must know who the user is.

To determine the prevalence of widgets and how they collect information, the Journal asked Brian Kennish, a former Google engineer, to examine the 1,000 most-popular websites, as ranked by Google's advertising network. Mr. Kennish last year launched Disconnect Inc., which offers software to block data collection by widgets.

Mr. Kennish's study examined more than 200,000 Web pages on the top 1,000 sites. He found Facebook obtained browsing data from 331 sites, and Google obtained data from 250 sites, some of it from its Buzz widget. Twitter got browsing information from about 200 sites.

Social-sharing widgets first appeared about five years ago, when online services such as Digg Inc. allowed users to share news articles. At the time, widgets did not cause browsing data to be collected by social sites. Widgets are installed by website owners, who like them because they can help generate more Web traffic.

Last year, Facebook introduced the "Like" button and other "smart" widgets. The widgets work with cookies that Facebook places in a Web browser when a user creates an account or logs in to its site. Together, they allow Facebook to recognize its users on any site with Facebook widgets.

Bret Taylor, Facebook's chief technology officer, says the technology lets websites show visitors what articles their friends liked, for example. "We don't use them for tracking and they're not intended for tracking," he says.

But Facebook says it still places a cookie on the computer of anyone who visits the Facebook.com home page, even if the user isn't a member. Mr. Taylor says Facebook uses such cookies to protect the site from cyberattacks by people who try to break in to users' accounts, among other things.

Until recently, some Facebook widgets also obtained browsing data about Internet users who had never visited Facebook.com, though Facebook wouldn't know their identity. The company says it discontinued that practice, which it described as a "bug," earlier this year after it was disclosed by Dutch researcher Arnold Roosendaal of Tilburg University.

Geoffrey A. Fowler contributed to this article.

Write to Amir Efrati at amir.efrati@wsj.com

Sponsored Offers

- Best Buy:
[Save 15% or more on the Best Buy deal of the Day](#)
- Walmart:
[Walmart coupon: \\$20 off your \\$50+ order](#)
- Wayfair:
[Up to 15% off + free shipping at Wayfair](#)
- Nike:
[Extra 20% off your purchase with Nike coupon code](#)

- The Home Depot:
[Free \\$20 Home Depot coupon with Pro Xtra membership sign up](#)
- Expedia:
[Exclusive Expedia coupon code: 5% off](#)

EXHIBIT 6

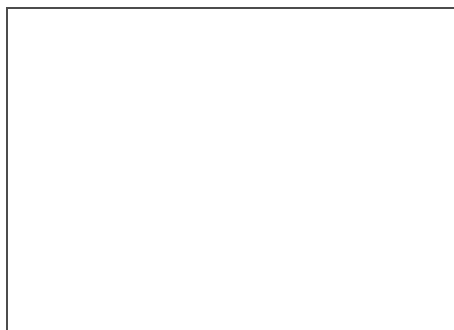
Facebook's New Privacy Bust: Users Log In but They Can't Log Out [Update]

Erik Sherman

[MoneyWatch Tech](#)



Updated on: September 26, 2011 / 5:37 PM / MoneyWatch



The biggest news at the f8 **Facebook** developer's conference last week was the [open graph](#) announcement. The company wants to expand its network of interconnections with other sites so people can see every more about what their Facebook friends read, hear, and see. [Virtually everything](#) would fall onto a Facebook timeline.

It's another example of Facebook's repeated privacy creep. Over time, the company keeps trying to learn more about all its users, pushing for a future where current notions of privacy simply don't exist. Now, depending on what apps and settings you use, it will be possible for [things you read and see to appear on Facebook](#) without your having to actually do anything. Not even click a "like" button. But it goes even further. Developer **Nic Cubrilovic** realized that [Facebook can track every page you read even if you log out](#) of the site. That means there is no getting away from Facebook tracking for many people.

Not-so-sweet cookies

Cubrilovic first noticed odd things about Facebook last year. As part of a development project, he had to create multiple profiles on the service. He'd log into one, log out, and then use another. Facebook would start suggesting the various fictitious people as possible friends. The service sets cookies that identify the browser to Facebook after sessions.

Leaving a cookie for later use is nothing new on the Internet. Nor is associating a particular account with a given computer and browser. Advertising networks do it all the time.

A [Facebook spokesperson pointed to an engineer's comment](#) on our sister site **ZDNet**, who said that the cookies are used for various reasons, but not for tracking people. Perhaps that's true. Perhaps not. The company has yet to provide an official statement on the issue, and one engineer might not know everything done by the site. Also, any statement that Facebook does not "share or sell" user data may be technically correct. But the company can still use the data internally to better

direct ads.

[**Update:** A Facebook spokesperson emailed the following statement:

Facebook does not track users across the web. Instead, we use cookies on social plugins to personalize content (e.g. Show you what your friends liked), to help maintain and improve what we do (e.g. Measure click-through rate), or for safety and security (e.g. Keeping underage kids from trying to signup with a different age). No information we receive when you see a social plugins is used to target ads, we delete or anonymize this information within 90 days, and we never sell your information. Specific to logged out cookies, they are used for safety and protection, including identifying spammers and phishers, detecting when somebody unauthorized is trying to access your account, helping you get back into your account if you get hacked, disabling registration for a under-age users who try to re-register with a different birthdate, powering account security features such as 2nd factor login approvals and notification, and identifying shared computers to discourage the use of 'keep me logged in'.

The statement develops some serious holes under analysis, which is what led me to send the following questions to Facebook:

- Do your open graph partners have the ability to read and interpret the cookies?
- Do they send information back to you?
- How can you show what friends liked if you don't keep a record of what they've done, which would seem to be the same as tracking?
- How can you measure click-through rate of users using "cookies on social plugins" if someone isn't monitoring who is doing what and where it's happening?
- Since your system often does know who the person previously logged in was and is looking for a password, how is that not the same as staying logged in? That is, still knowing who the person is?
- If you don't use any information from social plugins to target ads, what do you do with the information?

I'll pass on any useful answer that I get.]

What makes this question particularly thorny is how interconnected Facebook seeks to become with so many other parts of the Web, and how an [increasing number of major sites](#) that will modify their apps to connect with Facebook's Open Graph. Here are a few that announced with Facebook:

- **The Guardian**
- **Hulu**
- **The Daily**
- **The Independent**
- **Netflix**
- **The Washington Post**
- **Yahoo**

Sorry, that's not how it works

Many who use Facebook who don't like the idea of other sites reporting information back have typically logged out of the system before going elsewhere. (I know I have.) What Cubrilovic argues is that [this does no good](#):

But logging out of Facebook only de-authorizes your browser from the web application, a number of cookies (including your account number) are still sent along to all requests

to facebook.com. Even if you are logged out, Facebook still knows and can track every page you visit. The only solution is to delete every Facebook cookie in your browser, or to use a separate browser for Facebook interactions.

When users log out, Facebook still leaves cookies intact that identify users as particular members, even though the site may say that you have logged out. Effectively, you don't get to log out.

Interestingly, Cubrilovic claims that he tried for a year to talk to Facebook about this, only to get no response. He says he finally went public with it because of the potential privacy issues with the company's announcements last week. If so, it wouldn't be that surprising. Facebook is a company that makes money by helping advertisers to use consumers' personal information to better target marketing. It loses information if someone can log out.

When you have to remember what *not* to share

As **Dave Winer** notes, there's an intrinsic ethical difference between [using information people post about themselves and seeking out other data](#) that you can find by following them. If you can track someone from site to site, it's as though you followed them in an unmarked car and took notes about everything they did.

The practical problem for many is that without the explicit step of posting something onto their accounts (and that can happen in some cases just by clicking a like button), they could easily forget that everything -- *everything* -- on a given site could go hurtling back to become public knowledge. What if they were reading about finding a new job and their bosses were connected through Facebook? What if they had some medical condition they didn't want widely known? Too bad and too late: it's already out there.

Related:

- [Facebook's Dilemma: Its New Features Are All About Zuck's Life, Not Yours](#)
- [LinkedIn Pushes Its Users Into Ads Because It Can \(and Wants That Money\)](#)
- [Technology Has Become the Marketing Snoop's Scapegoat](#)
- [Desperate Groupon Tries to Fix Finances with Consumer Privacy](#)
- [Facebook's 5 Step Plan to Ignore Privacy and Collect More Personal Data](#)

Image: morgueFile user [duboix](#), site standard license.

[Erik Sherman](#)

Erik Sherman is a widely published writer and editor who also does select ghosting and corporate work. The views expressed in this column belong to Sherman and do not represent the views of CBS Interactive. Follow him on Twitter at [@ErikSherman](#) or on [Facebook](#).

[Twitter Facebook](#)

Thanks for reading CBS NEWS.

Create your free account or log in
for more features.

Please enter email address to continue

Please enter valid email address to continue

EXHIBIT 7

Facebook's CEO Mark Zuckerberg F8 2014 Keynote (Full Transcript) – The Singju Post

Pangambam S



Exhibit
Klein v Meta
Jackie Chang
1302

Mark Zuckerberg at F8 2014 Keynote

Facebook held its 2014 f8 developer conference at The Concourse in San Francisco on April 30, 2014. Mark Zuckerberg, Facebook's founder and CEO gave keynote address at the event along with other management team members of the company. We produce here the full transcript of the event...

TRANSCRIPT:

Mark Zuckerberg – Founder & CEO, Facebook

Welcome. Welcome. Thanks for coming to F8.

This is going to be a different kind of F8. In the past, we've had F8 when we had some kind of big new product announcement or new direction that we were going in. And this always meant a lot of different changes for your apps.

Now we're focused on building a stable mobile platform. You're trying to build great mobile apps and businesses and we want to bring this community together once a year to talk about all of the different things that we're doing to help support you.

Stable Mobile Platform

So we've heard from you that you want to use Facebook platform for three main things: to help you **build**, **grow** and **monetize** your apps. You want things like identity and sharing, push notifications, app installs, ad networks, and the best way that we can help you improve people's lives and help connect the world is by providing you with a stable mobile platform to build, grow and monetize your apps.

So we're going to help you build with tools like Login which are now used by more than 80% of the top iOS and Android apps. We're going to help you grow with stable distribution, like the more than one billion app installs that we've driven to your apps. And we're going to help you monetize and build stable businesses, like the more than \$3 billion in payments that we've helped process for you in the last year alone.

So most of you are building mobile apps. And over the past few years, we've made this transition to being a primarily mobile company ourselves. Just a few years back, most of our business and most of our usage was on desktop. But now more than a billion people use all of our mobile apps and more than 20% of all time spent in apps on phones is spent in Facebook apps and the majority of our business is on mobile.

But the thing is it can be annoying to build for mobile because the mobile ecosystem is so siloed. Apple has a vertical platform; Google has a vertical platform. Microsoft has a vertical platform. Then there's the mobile web and there are others too. And these are all important platforms and they're each growing.

But the thing is all of these companies are just trying to compete and make their own platforms better and more different from the others. No one has an incentive to help bridge the gaps between these platforms and make it easier to build on any of their competitors' platforms.

But as a person using a phone, this is terrible. I just want to be able to buy a phone and have all of the apps that I want worked on it. And as developers, of course, we want tools that work across all these different platforms. It's really annoying when we have to build the same thing three, four, five times just because of these different stacks.

So our goal with Facebook is to build the cross-platform platform and provide all the tools that you need to bridge these different worlds. So we all want identity across platforms and sharing across platforms and push notifications across platforms and app installs and even monetization. And this is what Facebook platform is all about – building the cross-platform tools that you need to build, grow, and monetize your apps everywhere.

Now it's natural for us to focus on these things because a lot of these tools are the very same things that we've needed to build for ourselves in order to help more than a billion people connect across all these different systems.

Now as I said, we're really focused on building a stable mobile platform. And one thing you may not know is that all of our own mobile apps are built on top of the very same platform and APIs that you guys use when you're running for Facebook. And all of our engineers use the same tools and read all the same documentation that you do.

So because of this, over the past few years as our apps have grown, the number of requests that our platform handles has grown by 20x. We know handle almost half a trillion requests a day, which is a pretty ridiculous number when you think about it. And the thing is when we've scaled, we've actually improved performance by more than 40% on average response time and we've reduced the already small amount of downtime by more than 70% over the past few years. So it's really important for you and for all of our teams internally that we build stable and efficient infrastructure that you can rely on for the long term. This has been a really big focus for us.

We used to have this famous mantra: *move fast and break things*. And the idea here was that as developers, moving quickly is so important that we were even willing to tolerate a few bugs to do it. But what we realized over time was that this actually wasn't helping us move faster because having to slow down and fix these bugs was slowing us down more than we were actually improving our speed.

So in the recent years, we've actually changed our strategy for moving faster. And now what we do is focus on building the best tools and infrastructure in the industry to build on top of it. So **move fast with stable infra** – it may not have quite the same ring to it, it may not be quite as catchy as move fast and break things. But this is – it helps us build better experiences for all the people that we serve and it's how we operate now.

So with this theme in mind, I want to start today by going through a few things that we're doing to make our platform even more stable and reliable for you to build on top to build, grow, and monetize our apps.

Now one problem that we all have is we write apps and we want them to run on lots of different phones, including older platforms. So you want to be able to build something you just know that it's going to be able to work for a while.

So today for the first time, we're introducing a two-year stability guarantee for all of our core APIs and platforms, including Login and Sharing. So this means that even if we change this core APIs in the future, we're guaranteeing that we're going to keep supporting them as is for at least two years and maybe longer from the time that we make that change.

Now we're still going to experiment with new features and different things but we're going to clearly mark those as beta so you know what's going to be part of this core stable platform.

We're also introducing **API Versioning**. So this is something that you know we want to make sure that all the apps that we all wrote two years ago keep working and this is something that we wanted internally as we built on top of this platform. So now every API that we launch is going to be versioned and you're going to get to decide what version of the API you build against.

We're also introducing an SLA that we're committed to fixing all major bugs within 48 hours. And this is something that we've always tried to move fast on and the reality is we're usually even faster than this. But now for the first time we want to put in place a firm commitment that we're going to be able to fix all these bugs or major bugs within 48 hours.

So with all these things, we think that we can produce an even more stable mobile platform; all these things that we're doing – hardening our platform for our apps, improving performance, introducing a stability guarantee, adding API versioning and adding a bug's SLA, we think we can help you ship even more great apps. So stability is the first theme that we're going to talk about today at F8.

Putting People First

Now I am going to change gears for a moment. Another big theme for today is going to be putting people first. We serve a lot of different communities here: developers, advertisers, employees. But one community is by far the most important out of everyone that we serve – and that's the people who use our products. And if you think about it – the reason that we're all here is really because of that. So it's really important in every single thing we do, we always put people first.

And over the years one of the things we've heard just over and over again is that people want more control over how they share their information, especially with the apps. And they want more say in control over how apps their data. And we take this really seriously because if people don't have the tools they need to feel comfortable using your apps, then that's bad for them and it's bad for you. But it will prevent people from having good personalized experiences and trying out new things but it also might hurt you and prevent you from getting some new potential customers. So we need to do everything we can to put people first and give people the tools they need to build a sign in and trust your apps.

Now we know that some people are scared of pressing this blue button. You probably – a lot of you have maybe even had personal experiences where you felt this. It's some of the most common feedback that we get on our platform. And the reality is if you're using an app that you don't completely trust or that you're worried might spam your friends, then you're not going to want to give it a lot of permissions.

So last year we took the step of separating out read and publish permissions to make it so that apps can no longer require you to give them the right to publish to other friends, all your friends in order to sign into an app. And I think this was a really important step and it helped people trust the blue button and trust signing in to apps. And today we want to do even more to put control and power back in people's hands.

So now whenever you sign into a new app with Facebook, you're going to see this dialogue. And if you want, you're going to be able to easily change line by line what you share with this app. So in this case, I want to sign in but you know I might not be comfortable yet sharing my email address or revealing exactly how much I love **Lana Del Rey** or maybe I just don't want to listen to **Summertime Sadness** on repeat right now. You know whatever the reason is – I don't talk about it right now; it's fine. I can just uncheck these boxers and I am done. With the new Login I can sign in on my own terms.

And if I don't want to edit anything here, then I can sign in with exactly the same number of taps that took before. There's no extra friction. So as a developer, this is going to help more people be comfortable signing into your apps and engaging with them.

Now we've heard really clearly that you want more control over how you're sharing with apps. And this new Login is all about giving you that control but we've also heard that sometimes you can be surprised when one of your friends shares some Azure data with an app. And the thing is we don't ever want anyone to be surprised about how they're sharing on Facebook and that's not good for anyone. So we're going to change how this works.

And in the past, when one of your friend blogged into an app, in this case Ilya, the app could ask him not only to share his data but also data that his friends had shared with him – like photos and friend list here. So now we're going to change this and we're going to make it so that now everyone has to choose to share their own data with an app themselves. So we think that this is a really important step for giving people power and control over how they share their data with the apps. And as developers, this is going to allow you to keep building apps with all the same great social features while also giving people power and control first. So I am really happy that we are doing this.

Okay. There's one more Login product that I want to talk to you guys about today. *How many times have you installed an app and wanted to try it out but you haven't wanted to create a brand new account or you're not yet ready to sign in with your real identity?*

Today we're going to solve this with a new service that we're introducing called **Anonymous Login**. And the idea here is that even if you don't want an app to know who you are yet, you still want a streamlined experience for signing in that removes the hassle of filling out all these different fields. So here's how it works, you can kind of see. This is what you're going to see the first time that you tap on the Anonymous Login button and of course after subsequent times it's just a one tap experience to get in. So you want hassle-free way to log in and try apps.

You probably also want an experience that can be synced across devices which is possible because we will provide an anonymous identifier even for not telling the app who you are. So you're going to be able to have an experience that sync without the app actually even knowing who you are for the first time. So this is going to let you try apps without fear and then if you want, you can always sign in with your real identity to personalize the app a bit later on once you're more comfortable using that app. So that's Anonymous Login. We're really excited about this one too.

So the new Login and Anonymous Login are examples of putting people first in the way that we designed this platform. By giving people more power and control they're going to trust all the apps that we build more and over time use them all more and that's positive for everyone.

These login tools are also examples of the kinds of cross-platform services that make up Facebook platform. Our place in the world is to build the stable mobile bridge across all these different worlds and these are just a couple of the examples of the type of things that we're building to do that. So now we'd like to walk you through all the other things that we've been working on to help you build, grow, and monetize your apps. And to do that, I'd like to hand it off to Ilya Sukhar to take us through the Build pillar of platform. Thank you.

Ilya Sukhar – Founder and CEO, Parse

Thank you, Mark. As I'm sure many of you know building things is hard. Building a product is hard. Building a customer base is hard. Building a scalable business is very hard. And every time the world of computing gets a little bit more exciting, a little bit more magical, new technology, new devices, the challenges for developers increase, there's new programming languages, new platforms, new devices, new versions, new things to think about.

And so the Build pillar of the Facebook platform is all about helping developers meet these challenges by leveraging Facebook's infrastructure, resources and footprint on every major platform. One of the things we're really excited about offering is Parse.

My cofounders and I started Parse about three years ago. And we found the process of building apps to be painful and tedious. We're reinventing the wheel over and over again with things that every

app needs, infrastructure, functionality that doesn't differentiate one app from another. No consumer actually notices the stuff, it either works or it doesn't and you certainly notice it doesn't and that's no good.

What am I talking about? Well, on the back end, there's things like servers and databases and APIs. On the client side there's all sorts of boring stuff – things like data models and sessions and caching and networking and you have to do this for every platform for iOS, for Android, for Windows Phone, for the web, for every version of Android, for every version of iOS, for every Phone out there, for every network out there, it's crazy.

Then finally there's your app – the thing that you care about, the thing that's different, the thing that's unique, this is the thing that you should be focused on. This is thing that matters. You might have some engaging UI, some unique content, some amazing functionality that's different, the thing that matters. And that's what Parse is all about. We make it easy to focus on that – the thing that will actually get you users and maybe even make you money – the thing that matters. And Parse takes care of all of the rest. You don't have to reinvent the wheel over and over again.

So we have three products. We have **Parse Core** which takes care of your data, your servers, your user accounts, your operations. We have **Parse Push** – gives you targeted fast push notifications for any device, for any platform. You don't have to think about which thing people are carrying in their pockets whether it's a tablet, a phone, whatever it is. And then we have **Analytics** to help you understand what's going on with your app and how your user base is doing. These are all the things you need to actually get your app off the ground and focus on that one important slice – the actual app.

Let me show you how this works with an example. These are the beautiful F8 apps. I hope you've all downloaded them. If you haven't, you can do so after I get off stage. Maybe after my colleagues get off stage. The core functionality here is pretty straightforward. It's the schedule. You can see what's going on for the rest of the day and you can favorite certain talks and get a personalized schedule so you can know where to be at any given time. Pretty cool, right?

So let me show you how Parse works and how it enables this app. Let me show some code. This is four lines in objective-C. I don't know how many of you guys have built iOS apps or just have used objective-C in another context. You can't do very much with four lines in objective-C. You can barely write your own names to the screen with four lines objective-C. It's really not that distinct but these four lines of objective-C are special. These four lines are Parse Core. And in these four lines, we can persist the fact that a user has favorited the talk. We don't think about servers, databases, networking, caching, schemas, any of that stuff, all of those things that are listed – just four lines of code. It's really that simple. You can do incredible things with just a few lines of code.

Parse Push – similar, this time in Java, little bit better. Eight lines. In these 8 lines, let me send a push notification to everyone within a mile of this auditorium, it's probably late, hurrying over here to hear me speak, or to hear Mark speak probably.

And **Parse Analytics** – in just a few lines of code, we can track what talks are reviewed and what people thought about them. And then I can slice and dice this in my dashboard to my heart's content. We have all these tools to build great apps across every single platform. We have iOS, we have Android, Windows Phone, we have Unity, may be building a cross-platform app across all of them, including Facebook Canvas, we have everything you need. So wherever you are right now and wherever you're going in the future, you can rest assured that we have the platform available for you there.

So we joined about a year ago. It's been an awesome year. It's crazy that it's a year. We came in the door with 60,000 apps and that was pretty cool but now we have 260,000 apps – almost tripled our user base and have served so many more apps. We've boarded over 140,000 new developers – everywhere all over the world. So if you're one of them, welcome, excited to be working with you. We're going to build some awesome stuff and you're not going to have to think about all of the nitty-gritty.

If you're not and you're still thinking about it or this is the very first time that you've heard of us, take a look at all these companies using Parse, all kinds of verticals, all kinds of use cases. We've got folks like Samsung, multinational corporations, TV networks like Showtime, gaming companies like Clarium and travel companies like Orbitz. It's not just Silicon Valley start-ups, or at least plenty of those as well.

So if you're two guys cooking something up, I am with you, I hope we can help you with their dream.

No matter who you are, I think you're going to like some changes we're making today. We've made our pricing radically simpler, cheaper and more predictable. We've expanded our free tier to make it even easier to get started with Parse and to grow on Parse as you get bigger and better.

Parse Core now offers unlimited API requests up to 30 per second for free. Parse Push now offers unlimited push notifications to up to a million people. That's a lot of people. If you need more of that, you just log into our dashboard and change a little slider. And Parse Analytics – very simple, just plain free forever. So if you're an existing customer and you have a bill coming, I think you'll be pleased it's going to be a little smaller or a lot smaller.

If you're not, if you're just getting started, you're thinking about using Parse, you don't have to pay us until your app gets huge and so we're aligned with you. We're excited about your app and we hope that it does get huge.

Speaking of Analytics, I like to start showing some new things that we build today. Spent a lot of time focused on our product and growth analytics are key to building your app and understanding where it's going, how people are using your app and whether they're coming back day in, day out.

Let me show you two of the dashboards we've added. So this is the growth dashboard and it tells you how your app is doing. Are people coming in the door? And you can see here that my app has done pretty well. I had great month of growth. Last week, though, not so hot. My streak is over. So I need to go back to what I was doing two weeks ago, whether it's great marketing, feature development, mobile app adds, something was working and I need to do more of that. This kind of data helps you understand what's going well and what is it? We're really excited about offering it.

And once you have people in the door, you need to understand – are they coming back? Are they coming back the next day? Are they coming back the next week? Are they coming back the next month? You can't just have a lot of growth. People might just go straight out the door. You want to keep them there. And so on this dashboard, you can see how that's going.

In the top right corner here, you can see that of the people who signed up 28 days ago, only 15.8% of them are still around, not so hot. I've got a problem there. So I need to do something about that. But you can see that on April 26, I did something right. I pushed a new feature, fixed some bugs, maybe changed my onboarding flow, something is going better. I need to do more of that. So I can understand what's affecting my users and what's bringing them back day in, day out. We're really excited about this and we're really committed to having the best mobile focused analytic solution out there. So look forward to more stuff from Analytics.

So I am going to change gears a bit. We've all been here, maybe we're settling into a long flight or struggling to get a connection at coffee shop, to check our email, there's times when we just don't have a connection, or it's really flaky. So you know what I'm talking about.

And so what happens? I'll show you. Your phone falls apart. Suddenly you're left with a calculator, a clock, gigabytes of space to jot down amazing frustrated notes. It's not quite a phone anymore and it's not quite that magical device that enables everything. And so why is that the case? It's not possible to build great apps that work well offline, it's just really hard and most developers start out small. So they don't have the resources, they wait until they have more. And so by and large only the best largest companies focus on this and everything else doesn't work quite so well. And for many people this is frustrating – it's frustrating for me, it's frustrating for that guy but for many people this is the default. People are just coming online and for them offline is the default. They occasionally get connectivity. And so we need to do better by that. We need to make it easier to build great offline apps.

So I am excited today to announce Parse Local Data Store. We're making it easier to build apps with Parse that work as well offline as they do online – it's a big set of improvements or SDKs. And it's just a few lines of code just like everything else. This is what it looks like, drop it in, type in some code and suddenly your queries work well offline. And we hope that this allows people to build amazing apps for the entire world, for the people who are waiting at the coffee shop or who are just getting online and only have a phone and a connection every once in a while.

So those are the Parse updates, we've grown a bunch, we've got new cheaper, simpler, more predictable pricing. We've new analytics stuff to understand how your app is doing as people are coming back. We've got great offline enabled SDKs. Check everything out at **parse.com**.

URL

Now I want to talk about something near and dear to my heart and hopefully near and dear to yours. The URL. I've been working with the URL for as long as I can remember. The URL is just beautiful. It made the web beautiful. The web is still beautiful. And the URL is the fundamental unit of sharing. I remember using the URL and sending it to people on email on IRC, on ICQ and AIM, on Facebook certainly and even MySpace, I mean every communication platform that has existed, still exist, will exist is going to use the URL. And it's a shame that it's not really a big deal on mobile right now.

Why is that? Let's take a look. We've got all these apps but they're stuck in their own silos. So Quip is one of my favorite apps these days. It's a great mobile enabled document editor. So I use it to collaborate. I use it to share things with my friends and family to plan things and when people paste weblinks into the document, it works great on the desktop, you click it, it's just like we've been doing for decades. The browser opens up and I do my thing.

But when I open up links that are going to say SoundCloud for music or Goodreads for books on my iPad, what happens? Well, I get stuck. I get stuck in a mobile web browser. I get stuck logging in. I

probably can't even listen to the music. I can't get actually what I want to do.

And so why is that? It's not because they're bad programmers. I think they're actually really amazing programmers over at Quip. But the world of mobile has no unified way to discover links, no unified way to navigate to links across all the platforms and to go straight to the locations in mobile that you want to get to that have the actual contact, the thing that you want to actually do with your life.

So that's the problem. What if that wasn't the case? What if we could break down these walls, free these apps from the silos and make it one big graph of content? What if we could make it really easy for developers to link to their — to other apps, send their users to the right place and get their users back so they can get on with their lives, after they've listened to that song or looked at that book, or booked that flight, whatever it is.

So we've been working on it and I'm excited to announce **AppLinks**. It's an open standard with a set of Open Source SDKs that solves all of these problems — gives you everything you need to publish, discover and navigate to deep links on mobile on any platform.

So let me show you how Quip is using it right now to enable my scenario and to make it so much better. So here I am. I am going to tap on Quip and this is a document I have been working on. There's some books, some poems, and some music. So I am going to click on that link. It's a mix — digging it — I am going to keep playing, and I am going straight back to Quip. All right, I have read this book but I still want to go in here and read it, now straight back to Quip. I am going to take [inaudible] for this, I am going to go for this poem.

There it is. It's pretty deep, feel different I'm going to star this. That's AppLinks.

What if every app worked like this, what if we never got stuck in mobile web browsers? Well, I'm excited to show you this.

So for developers, pretty simple — a set of new tags that you can drop into your content, if you've got a website, tells folks where your iOS version or your Android version, any other version that you have of that content. If you don't have a website, you're mobile only, we've got a special API for you, you can also use Parse, you can use any other service that's out there. It's really simple.

We also have a new API that translates between any web URL and the mobile equivalent, so you pass at a web URL and you get back whatever mobile versions are available. And so we crawl the web for you, you don't have to do it but if you want to, you can. It's an open standard. We invite other people to bring up these kinds of indices.

And lastly, our open source SDKs that you can just drop in have one line of code to send your user over to another app to give it all the contacts that needs to send it, send that user right back to where they came from and that's it. Whatever platform you're on, it's one line of code, super simple.

And we're really excited that we've partnered with a lot of great partners. We've got great content available today for you to link to. So if you have an app that could benefit from looking to Hulu or to Pinterest, or to Vevo or to any of the other — these other great partners, you can start linking to them today. They've made all of their content available via AppLinks.

We have also adopted this. So the iOS apps, the Android apps that we have now use AppLinks. And so we'll deep link into your app when appropriate. That's pretty cool.

And lastly I'm super excited that some people have already taken to this and are really expanding this ecosystem deeply. We have folks like Mailbox who are baking the straight into their apps. So when you're reading emails on your iOS app, you can go straight to the other app, whether it's a house on Redfin or a song from Spotify, go check it out and go straight back to your email and get on with your life. No more logging in.

Spotify is working with Songkick to make it really simple to just buy concert tickets, listening to a track, you like the artist, you want to see if there's a concert there, you hop over to Songkick, tap a few things, it's got your credit card already and you hop right back. You're back to listening to music. And so I hope this is the direction that mobile takes for the future. This is how the web worked and it's awesome. Let's keep it awesome. Everything's available on AppLinks.org. It's all open, it's all open source, so if you have contributions, comments, we'd love to hear them, we love to work with you to build a stable foundation for the future of mobile and to make everything more open and connected.

With that, I'm going to bring up Ime to talk about the next section. Thank you.

Ime Archibong — Product Partnerships Director, Facebook

Hi everyone. My name is Ime Archibong. I lead Strategic Partnerships team here at Facebook. I get to work with a tremendous amount to you and also the developers around the world. I also spend quite a bit of time coaching kids to basketball and one of the more frustrating moments of coaching kids to basketball is when you have a kid coming to you and say, "Hey, coach, I want to take my game to the next level. I want to get recruited. How do I stick out from the rest of my peers". It's a frustrating moment for me because I know the one thing that they need is the one thing that I actually can't provide or teach them. Can't teach a kid how to grow, just can't do it.

In fact, similarly many of you struggle with growth challenges but thankfully when I have those conversations, they end a little more optimistically with you. Conversation starts off the same. You're asking — so similar to kids, you guys are asking how do you stand out from your peers? How do you stand out from the two million apps that exist across the App Stores? And ultimately how do you grow?

But that's when I get excited, because I know that Facebook has always been committed to building tools and services and channels both organic and paid to help you take your app to the next level, help your app grow. So I am going to talk through a couple those. But let's start with the organic tools.

So most of you are familiar with these. I want to talk a little bit about the evolution of these great organic tools to the mobile ecosystem that will hopefully help you build better app experiences, accelerate your growth and also solve some of the problems that we've been talking about for a number of years.

So what are those problems? A number of you still have a tremendous amount of people visiting your web experience every single day. And there's nothing wrong with web traffic by any stretch of imagination. But these are the same users that you hopefully would want engaging with your native mobile app, especially if mobile is where your product roadmap is focused, especially because mobile is going to be the thing as you're driving your growth in the future.

So as a solution, we built Send to Mobile which is a quick and easy way to start to funnel some of that desktop traffic to your native mobile experience. So let's say I am in the Rdio app, I am logging in via Facebook on the web, Send to Mobile will send a push notification to my Facebook app, so next time I fire it up, it will remind me to download that Rdio application. The benefits here are really, really clear, right? I'm not searching through the two million apps to try to find your application and hopefully you've now converted what is a good desktop user and to engage mobile app user. And that's where you want them in mobile but it doesn't necessarily eradicate all your problems.

Let's talk about the next one. You have this engaged mobile user but you really want to arm them with the tools that they have been using for the last several years to essentially share your content, your app back with their friends on Facebook. Historically we've done a great job of doing this through social plugins and in particular the Like button which you're all familiar with. The Like and Share button in fact actually are used across over 10 million websites today.

So many of you rightfully so have been asking when are we going to bring this to mobile? So it's finally here. I'm excited to announce the Mobile Like button. The Mobile Like button is a great way to get a user who's either logged in the Facebook on your app or not to share their content of your app and your app back with broadly with their friends across Facebook to send and tag friends app. And they've added Mobile Like button to this article. An easy lightweight way they've empowered me to be an evangelist for their app, their app's content with a broader from my friends across Facebook. Mobile Like button is currently available to be rolling out over the next couple of weeks.

So now you have someone that's engaging your mobile application. You've also given the power to share more broadly with their friends across Facebook but you still have one more problem. People want the ability to share privately with a close group of friends or maybe just one on one with a brother or sister.

So the last new organic tool is the Message Dialog which is a quick and easy way for people to share your apps content through the messenger app. So to take, for example, if I was strolling through the Vevo app, looking at music videos and I come across this great Lana Del Rey track. Similar to Mark, I probably don't necessarily want to share with all my friends but I want people that love and appreciate her music too that don't understand it now — so at one tap of the messenger button, the Vevo is built here, I can privately intimately and share this video with a close group of friends, including Mark, the nice reminder to let him know not to share more broadly with all our friends and keep it close to chest.

So these three new mobile tools help fix a number of challenges for you. Many of guys are startups out there and conversations with you, we're really sensitive to the challenge that you have just to operate your business. And what I'm talking about here is the product management tools you need, the marketing help you need, the communication tools that you've been looking for, that stuff is critical and it all adds up.

So today I'm really, really excited to announce a new program that Facebook has put together with a group of partners to help you with these needs. The program is called **FB Start**. This is a program that's going to provide you with up to \$30,000 in free tools and services to help you get your app off the ground and running fast.

So alongside of Facebook and Parse, there's about 11 other great companies that have come to the table to bring you this program. There's Blue Jeans for your communication needs, MailChimp for your marketing needs, Salesforce for your customer service needs, and Appurify for your mobile testing needs. All of these partners truly believe in supporting startups and making sure that you can

focus on the thing that you need to do and you want to do to build great products.

If you're a start-up, there are two tracks that you should know about with FB Start. The first is **Bootstrap** which provides about \$5000 of these free tools and services to help you get your app on and started. If you already have a product out there, you're seeing some early growth, the question is how do you celebrate that?

So the **Accelerate** track is for those of you that have a product out there. It's worth about \$30,000 of these free tools and services.

So if you're in the audience today, we're opening this up right away for folks that have registered for f8. Feel free to go to this link and apply and we're rolling out more broadly over the next couple weeks. I'm truly excited about FB Start and what it's going to bring to the startup community.

So let's transition over to the paid tools for a second. For years, many of you have asked, "Hey, how can I find the right person on Facebook where they're engaged the most? So couple years ago, we launched **Mobile App Ads** which enable you to take the power of growing directly into your own hands. These mobile app ads are helping you find the right person once again where they are most engaged which is their mobile Facebook News Feed.

So let's look at an example in the real world. Facetune, an Israeli start-up that built a great app that helps you tweak and tune your photos before you share more broadly with your friends on Facebook. Personally I use them to edit selfies, not too much, nothing too major but just a little tweak here and there to make sure that my smile sparkles. With little resource this company had, it really embraced mobile app ads.

In fact, the results speak for themselves. These five entrepreneurs over the course of five days with only \$500 of marketing budget were able to take their app from 283 in the App Store all the way up to number two position. Additionally over across 78 different Geos and locations they skyrocket, it's the number one slot. 94 countries, the number one slot. Why not, let's add more.

But Facetune wasn't the only developer that saw great results using mobile app ads. In fact, many of you in this room did too, and thousands of other developers across the world. To date 350 million installs have been driven through this product. 60% of the top-grossing apps are also leveraging this product. So it's been really clear to us that we've been able to provide you with the strong powerful tool to efficiently find the right people on Facebook at scale.

Let me give you a even deeper and more personal example of what the right people mean. This is me. I love music, and I have never been shy about telling my friends on Facebook how much I love music. Over the course of the last couple years I've liked dozens and dozens of music-related Facebook pages, and it shows. So with the power of Facebook targeting, if you were a music app just getting started right now, there's no reason why you shouldn't be able to get your app in front of me on Facebook and had me download and install it.

But we all know the facts -- several people download these applications, they get buried on the seventh screen of your device, they never go back and revisit them. That's a problem. It's something that we've tried to go and solve. And our solution for that were Engagement Ads.

Engagement ads are quick and easy way for you to target someone on Facebook and bring them back into your app experience. You're able to target folks on a bunch of different factors but one of the ways that Facebook has actually recently been able to make you target folks has been In-app events. So In-app events — so these events that are happening in your app location that are unique to your app, only you know about them, we've now given you the power to target people on Facebook based off of these events.

So take, for example, if I download Beats music app, fantastic new app, couple weeks ago, I go through the onboarding flow, I've told them what genres of music I like, some artists that I like including Beyonce and Jay-z but then I got distracted. I got pulled the email or whatever it was but I was unable to revisit the app and really dive into the music.

Engagement Ads in a lightweight way has given Beats music the ability to target me on Facebook based off the fact that they know I've listened and I like Beyonce, and say, "Hey, listen now, we've got this great new fall playlists coming out and there are some great Beyonce tracks on it". For me personally, it just doesn't feel like an ad, this is like a nice reminder from a friend to go listen to some content I am really going to enjoy.

Yplan, a slick ad that curates the top events in any city. Recently we ran an Engagement Ad campaign for an upcoming rooftop party in San Francisco. It targeted people that were in San Francisco that installed the app already. Essentially told them and communicated to them to Book Now with one-click at the Book Now button, it's taken directly into the event in the app, was able to reserve my spot. Once again they saw solid results over the course of this campaign. A 20% increase in overall with paid bookings and a whopping 215% return on their investment. So these are meaningful stats for any size company, any size start-up, anyone who has an app out there.

If you want to learn more about our app products, feel free to visit this URL for more case studies and more information. So there you have it, some exciting new tools, mobile focus to help you grow. And whether the organic ones or the paid ones spoke to you the most, my hope is that you really just go put these tools to work. We've built them for you and we've built them with you.

There's one thing you take away from the last couple of minutes of this conversation is that Facebook is truly committed to building scalable, stable, people-friendly tools to help you grow and take your app to the next level.

With that, I am going to turn over to my colleague Deborah Liu to talk a little bit about making money.

Deborah Liu – Project Management Director, Facebook

Thank you, Ime. Hi, I am Deb Liu and I work on ads and payments for developers at Facebook. You know, I spend a lot of time talking to developers and a lot of them asked me beyond how to grow, it's how to make money. And that's really important because money is the lifeblood of your business. It's what helps you hire that next engineer. It's what helps you build that next app. It's just how you keep the lights on in your office. So I'm here to talk about **monetization** and how we can help.

We have been helping developers with monetization for years. Game developers have been building amazing immersive games on the Facebook platform, with beautiful graphics, beautiful experiences, something that I play every single day. And over the past five years, we've built a world-class payment system to help with monetization.

And we are really, really excited about the results. 375 million people play games on Facebook every single month. And over a hundred developers — 100 of you are making over \$1 million in our platform every year. And the stat I am most proud out is that we've had the privilege of processing \$3 billion in transactions on Facebook on your behalf.

We are really committed to the canvas business and making our developers on canvas a success, and we're continuing to invest and grow that ecosystem in the years to come.

Recently, we've been getting a lot of questions which is how do I make the shift to mobile. How do I make money on mobile? We are in a unique position to answer that question because, you know, just two years ago, we faced the same problem which is we made no money on mobile. We had the top app in iOS and in Android and we made no money from it. And we needed to solve this problem for ourselves but we couldn't just take our right hand side ad, move it to mobile. It's a different user experience, it's a different form factor, it just didn't make sense. But we had to figure it out.

Like lots of companies who go through these types of transitions, we faced a lot of challenges. But we came out with two important lessons. One, it's an advertising — traditional advertising still works on mobile and it works really really well. And two, is that we had to reinvent how Facebook looked with ad in it as part of the user experience.

And two years later, here we are. Over a billion people are accessing our apps on mobile and we make nearly 60% of our revenues there.

So how do we do it? I don't know what you do first thing in the morning. But I check my Facebook newsfeed. And I check out what's happening but what people are talking about, photos of my friends and their family. And what I also see embedded in my newsfeed are beautiful and relevant ads. You know, I am the mom of three young children under seven, and they grow out of their clothes constantly. And you know when I see an ad for discount clothes, beautiful quality, I click and I buy. And that's what Facebook ads are about, which is it's just like our newsfeed, just like we connect people with people, the story of their lives, the things that they care about, the news that they share, we connect advertisers with people, the messages they're trying to get out there for people. And that's what advertisers are looking for. And what people on Facebook are looking for are ads that are integrated, not disruptive. And that's how we've made it work.

Over the past 10 years, we have built an advertising base of over a million advertisers who are coming to Facebook to set up their campaigns and find an audience. And we do that because we have the world class targeting system that allows them to find the exact audience they're looking for.

And so when an advertiser comes to Facebook, they set up their campaign and tell us who they want to find. And our system can find the person amongst the three of us who had Game of Thrones parties and the other who has three kids who sing the song Let It Go at the top of their lungs. Imagine our system couldn't tell the difference, how that would hurt the advertiser and the experience that people have on our sites. But you know, we've been able to solve that problem for advertisers and for people. And that's what makes it great.

We're bringing together the most demand, the best targeting system and today we bring you in. We're excited to announce the **Audience Network**. We bring it all together for you so that you don't have to go out there as a publisher and developer and hire giant sales team and sell app. You don't have to find out who in your app is the right person for right audience is. You don't have to parse your audience. You don't have to create reporting, you don't have to do billing, you don't have to figure out measurement on behalf of advertisers. It's all done for you.

How Audience Network Works

So let's take up a little bit on how it works. If you learned anything about mobile, is that formats really really matter and so let's say you want to use a banner ad. With a few lines of code, you can have a really relevant ads that come into your system. You can have the power of all of those campaigns brought to you, all of that matching, all that targeting, making into your app, so your ads rather than be interrupting to your experience are actually a part of the experience.

The same thing is true for **interstitial**. Again just a few lines of code to access all of that great inventory, and have your audience have relevant interesting ad. And if you want to invest a little bit more time, we encourage you to work with us on native advertising. We have pioneered the space on mobile and made advertising amazing because it's heart of the user experience. It is heart of Facebook.

Let's take a look at 3 examples. So Target came to us and they said, we want to find people who use our app already but who would also like to see the movie Frozen. You know, that's a really interesting target set and you know where we found those people? We found them on the Huffington Post and dozens and dozens of other apps. Target didn't have to go reach out to a bunch of app and Huffington Post didn't have to set up a bunch of campaigns for them either. It all came together to the Facebook system. It is the best experience for advertisers because they're getting their ROI that they're looking for. And Huffington Post has an easy time getting these ads in their system.

Coca-Cola came to us and they said, we would love to have people who look like the people who already use our app. We have a great audience, we really really love them, we want more of them. And they found that audience in Vinted – a vintage clothing site. Again Vinted didn't have to go out there to set anything up, it just came and it was really simple. And so as a developer, they're getting the best return on investments.

And finally, Audible came to us and they said, we want fans of Game of Thrones, because we want to get them to come and listen to Game of Thrones on our sites. They found that and cut the rope. And because the ads are relevant and interesting, you get better click-through rates (CTR), better returns on investment (ROI) for the advertiser and more money for the app. That's what we're bringing together today.

We have spent the last 10 years building up a base of amazing advertisers looking for an audience and audience is in your app. We marry that with the best targeting system in the world, and we're opening it up to you. Great ads that are really relevant to your people, helping you to make more money.

Sign up for the Audience Network today. We look forward to working with you.

Thank you. And now we will bring Mark back out.

Mark Zuckerberg – Founder & CEO, Facebook

Thanks, Deb. I'm really excited about this Audience Network. We've done a lot of work already in the past years to help you build and grow your apps. And this is really the first time that we're going to help you monetize in a serious way on mobile. And you know, the mobile ecosystem needs a way to deliver these kind of native personalized ads to people and I'm glad that we can help deliver more than a million active advertisers to you apps for you.

So build, grow, and monetize. This is what you need to build great mobile apps and great mobile businesses.

Now we've heard a lot of different updates today. But one thing you didn't hear was some completely new shiny directioner product from us, because today is all about listening to you and hearing the things that you want from our platform and deepening how we support you in these three fundamental ways – to help you build, grow and monetize our apps.

So keeping with this year's theme of stability and consistency, I want to close today by inviting you all to next year's f8. We're moving to Fort Mason which is going to be slightly bigger and a little bit cooler hopefully. But you can expect from now on for us to have f8 around the same time every year. It's a great opportunity to bring the whole community together.

Now I want to leave you with, with one final story today. This has been an interesting period – it's been a reflective period for me personally. We just reached Facebook's 10th anniversary as a company and in a couple of weeks I'm turning 30 – who doesn't like a birthday. And just a little while ago, I just also celebrated the 10-year anniversary of when I met my wife for the first time. So it's been this really interesting period to reflect on the past decade which has been amazing and what's important in life and things like family and Facebook for me in philanthropy, and you know what here for us for the next decade ahead.

And on Facebook's 10th anniversary we brought the whole company together and we talked about our culture. And we talked about how we have this really strong hacker culture at Facebook. Now it's helped us accomplish so much, helped us connect so many different people but we also talked about how our hacker culture is inherently focused on us. It's the way that we do things. It's not really that focused on the people we serve.

And you know, to reach the next level and to fully achieve this mission of helping to connect everyone in the world, my goal for our culture over the next 10 years is to build a culture of loving the people that we serve — that is as strong if not stronger than our culture of hacking at Facebook. And I hope that you can see the seeds of some of this today in what we're talking about. We want to build a platform that's reliable and stable for you. That's really important to us. We want to make sure that we put people first in all of the different experiences that we offer and ship. And we want to help you guys touch more people's lives.

We've already done so much together and I'm really confident this path forward is the way to connecting and improving every person's life in the world. It's an honor to serve you guys in this mission. Thank you for coming to f8 and I'm looking forward to seeing you work all together.

Please follow and like us:



20



EXHIBIT 8



Document (1)

1. [*Antitrust Law: An Analysis of Antitrust Principles and Their Application \(CCH\) 782*](#)

Antitrust Law: An Analysis of Antitrust Principles and Their Application (CCH) 782

Antitrust Law: An Analysis of Antitrust Principles and Their Application (Areeda and Hovenkamp)

> *Antitrust Law: An Analysis of Antitrust Principles and Their Application - Areeda and Hovenkamp* > *CHAPTER 7 Monopolization: Particular Exclusionary Practices (700-787)* > *7E Unfair, Predatory, and Tortious Competition Unrelated to Pricing Policies (780-782)*

782. Specific Tortious Practices

Last Updated: 5/2023

Specific Tortious Practices

782a.

Business torts generally.

In *Retractable Technologies*, the Fifth Circuit held that "disreputable" tortious conduct could not violate §2 and, further, that diverse instances of that conduct, which included claims of false advertising, could not be aggregated into a §2 violation either.¹ "This distinction between unfair conduct and anticompetitive conduct is critical to maintain because the antitrust laws "do not create a federal law of unfair competition or 'purport to afford remedies for all torts committed by or against persons engaged in interstate commerce.'"²

¹ *Retractable Techs., Inc. v. Becton Dickinson & Co.*, [842 F.3d 883 \(5th Cir. 2016\)](#), cert. denied, **137 S. Ct. 1349 (2017)**. See also *Northbay Healthcare Grp., Inc. v. Kaiser Found. Health Plan, Inc.*, [838 Fed. Appx. 231 \(9th Cir. 2020\)](#) (plaintiff adequately alleged monopolization in defendant's campaign to steer patients away from plaintiff's hospitals; dissenter believed that the allegations lacked specificity); *Right Field Rooftops, LLC v. Chicago Baseball Holdings, LLC*, [80 F. Supp. 3d 829 \(N.D. Ill. 2015\)](#) (denying temporary restraining order after finding unlawful monopolization unlikely in stadium's construction of billboards that interfered with plaintiffs' view of the game from adjacent rooftops and thus their business of selling access to such rooftops). A related decision concluded that the baseball exemption from the antitrust laws also applied. *Right Field Rooftops, LLC v. Chi. Cubs Baseball Club, LLC*, [870 F.3d 682 \(7th Cir. 2017\)](#), cert. denied, **138 S. Ct. 2621 (2018)**.

² [842 F.3d at 892](#), quoting *Brooke Grp. Ltd. v. Brown & Williamson Tobacco Corp.*, [509 U.S. 209, 225 \(1993\)](#), and citing 806d.

course, any competent retailer keeps its own sales figures, often via scanner data, and as a result has high-quality information about what is selling and what is not.

Finally, the court condemned the defendant's "consumer alliance program" (CAP), which entailed discounts of approximately .3 percent off the wholesale price in exchange for the retailer's provision of sales data and participation in the defendant's sales promotions, as well as giving the defendant preferred advertising space on display racks.¹⁷ The agreements were terminable at will. Condemnation of these agreements places the Sixth Circuit in conflict with every decision addressing the issue.¹⁸ First, the discounts were very small, and the resulting prices left the defendant with very high margins in the United States, which means they could readily be matched by any rival.¹⁹ The court did not insist on a showing that rivals could not match the discounts if they wished. Second, the discounts were not conditioned on exclusive dealing at all; they only concerned preferred shelf space access. Even absolute exclusive dealing would be condemned only after a finding of significant market foreclosure; in this case the plaintiff had not been excluded from any portion of the market. Third, the agreements could be abandoned by retailers at any time, meaning that any rival could compete for the business simply by matching the discount.²⁰

To the extent it is followed, the *Conwood* decision will lead to less aggressive competition and to higher prices in retail markets having a dominant firm. While some of the defendant's actions were undoubtedly tortious, the court required no attempt to segregate the effects of these from the effects of lawful conduct. More problematically, the court included in its

¹⁶ However, the court also cited evidence to the contrary, noting that Kroger's buying manager ... testified that any supplier trying to use category management practices to control competition, in his store anyway, would be "committing suicide." USTC points out that no retailer testified that the company required shelf space allocations equal to its market share. Apparently, Wal-Mart rejected such a request from USTC. *Id.* at 775.

¹⁷ *Id.* at 778.

¹⁸ See P768, P1807.

¹⁹ *Conwood*, [290 F.3d at 774](#).

²⁰ On the impact of contract duration on exclusive-dealing requirements, see 1802g. *Contrast Concord Boat Co. v. Brunswick Corp.*, [207 F.3d 1039 \(8th Cir.\)](#), *cert. denied*, **531 U.S. 979 (2000)** (dismissing complaint of anticompetitive discounting when buyers could forsake the discounts at any time).

condemnation actions such as providing integrated shelf space at a retailer's request, or doing so with its permission, provided that these actions were also accompanied by things such as rack displacements conducted without permission, relatively minor promotional discounts, and perhaps the provision of false information to retailers in a position to verify the information readily.

782a3.

Patent infringement as antitrust violation.

In *Retractable Technologies*, the Fifth Circuit held that an act of patent infringement could not be an antitrust violation.²¹ The logic of the plaintiff's claim was that the plaintiff was entitled to exclude firms from the portion of its technology that was patented but that the defendant had invaded this space by infringing the patent. Citing the small amount of precedent on the issue,²² the court observed that "[b]y definition patent infringement invades the patentee's monopoly rights, causes competing products to enter the market, and thereby increases competition."²³

Clearly, the court is correct on that point. Patent laws and antitrust laws have their own theories of harm, and the new market entry caused even by an infringer represents an increase in competition and thus is not "antitrust injury"²⁴ even though it is cognizable injury under the Patent Act. But that fact also invites an additional point, which is that the patent laws themselves contain remedial provisions penalizing patent infringement, also permitting significant damages for loss of sales or related injury. An antitrust court entertaining such a claim would have to determine everything that a court would have to determine in a patent infringement case. The difference, of course, is that by turning patent infringement into an

²¹ *Retractable Techs., Inc. v. Becton Dickinson & Co.*, [842 F.3d 883 \(5th Cir. 2016\)](#), cert. denied, **137 S. Ct. 1349 (2017)**.

²² *Northwest Power Prods., Inc. v. Omark Indus., Inc.*, [576 F.2d 83, 88-89 \(5th Cir. 1978\)](#); *Kinnear-Weed Corp. v. Humble Oil Ref. Co.*, [214 F.2d 891, 795 \(5th Cir. 1954\)](#).

²³ *Retractable Techs.*, [842 F.3d at 893](#).

²⁴ On antitrust injury, see P337.

antitrust claim the plaintiff could obtain treble rather than actual damages and attorney's fees, but there is no warrant in either the antitrust laws or the Patent Act for such an approach.

782b.

Misrepresentations or false statements.

A monopolist's misrepresentations encouraging the purchase of its product can fit our general test for an exclusionary practice when the impact on rivals is significant; deception of buyers can impede the opportunities of rivals. Even apart from its impact on rivals, deception is undesirable because it can injure buyers and offend public morality. There is no redeeming virtue in deception, but there is a social cost in litigation over it.²⁵

To determine the impropriety of a representation implicates the usual tort issues with respect to nondisclosure (When is there a duty to speak?), the distinction between "fact" and "opinion," the knowledge or due care of the speaker, the actual degree of reliance by those allegedly deceived, and the "reasonableness" of any such reliance.²⁶

That particular buyers might have been deceived is not itself of §2 concern. The buyer's injury is independent of the seller's power; to be deceived by a minor seller can be just as costly to the buyer as to be deceived by a monopolist. Of course, the effect on honest rivals might be worse when continuous deception is practiced by a monopolist than when practiced by one of many small firms in a competitive market.

²⁵ Advocating relatively broad liability is Michael A. Carrier & Rebecca Tushnet, *An Antitrust Framework for False Advertising*, 106 Iowa L. Rev. 1841 (2021) (arguing for a presumption that monopolists engaging in false advertising of the monopolized product violate §2, rebuttable by proof that the advertising was ineffective).

²⁶ Federal Trade Commission Act §5 empowers the Commission to order the termination of "unfair methods of competition ... and unfair or deceptive acts or practices." Misrepresentations and especially deceptive advertising are included. And although the Commission has not attempted to proscribe all "puffing," its prohibitory orders do not depend on showing that any buyer actually or justifiably relied on a false or incomplete representation. This may be altogether appropriate in an effort to lift standards of accuracy in public advertising by prospective orders against continuation of the conduct and without any other public or private remedies or sanctions. But such rulings cannot be applied automatically where serious additional sanctions would result. In all events, FTCA §5 cannot be enforced by private parties.

The key problem here is the difficulty of assessing the connection between any improper representations and the speaker's monopoly power.²⁷ The more typical deception defendant is the smaller firm or recent entrant that makes its false claims, collects the payments from deceived consumers, and then disappears or becomes judgment-proof. The false claim leading to or perpetuating durable market power by a firm capable of being sued is much less likely. Because the likelihood of significant creation of durable market power is so small in most observed instances-and because the prevalence of arguably improper misrepresentation is so great-the courts would be wise to regard misrepresentations as presumptively de minimis for §2 purposes.

The presumption could be overcome by cumulative proof that the representations were (1) clearly false, (2) clearly material, (3) clearly likely to induce reasonable reliance (4) made to buyers without knowledge of the subject matter, (5) continued for prolonged periods, and (6) not readily susceptible of neutralization or other offset by rivals.

The Second Circuit accepted these principles in its *Berkey* decision.²⁸ Kodak had introduced a new film, Kodacolor II, promoted its virtues, arranged demonstrations so as not to reveal the "red eye" of flash pictures for early batches of the new film, and indicated a 14-month shelf life although the film lost half its speed within three to six months. The court found no antitrust violation here:

A monopolist is not forbidden to publicize its product unless the extent of this activity is so unwarranted by competitive exigencies as to constitute an entry barrier. ... And in its advertising, a producer is ordinarily permitted, much like an advocate at law, to bathe his cause in the best light possible. Advertising that emphasizes a product's strengths and minimizes its weaknesses does not, at least unless it amounts to deception, constitute anticompetitive conduct violative of §2.

²⁷ See Susannah Gagnon & Herbert Hovenkamp, *Antitrust Liability for False Advertising: A Response to Carrier and Tushnet*, 107 Iowa L. Rev. Online 82 (2022), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3982240.

²⁸ *Berkey Photo, Inc. v. Eastman Kodak Co.*, 603 F.2d 263, 287-88 & n.41 (2d Cir. 1979), cert. denied, 444 U.S. 1093 (1980).

The Sherman Act is not a panacea for all evils that may infect business life. Before we would allow misrepresentation to buyers to be the basis of a competitor's treble damage action under §2, we would at least require the plaintiff to overcome a presumption that the effect on competition of such a practice was de minimis. ²⁹

Misrepresentations and organized deception by a dominant firm may have §2 implications when used against a nascent firm just as it is entering the market. Such a firm has no established customer base and typically lacks the resources to answer the dominant firm's

²⁹ *Id.* See also *Lenox MacLaren Surgical Corp. v. Medtronic, Inc.*, [762 F.3d 1114 \(10th Cir. 2014\)](#) (recognizing §2 claim based on dominant firm's telling potential customers that rival's product was dangerous, and helping to initiate a recall: "A Section 2 plaintiff may rebut this presumption by satisfying a six-factor test, showing that the disparagement was: (1) clearly false, (2) clearly material, (3) clearly likely to induce reasonable reliance, (4) made to buyers without knowledge of the subject matter, (5) continued for prolonged periods, and (6) not readily susceptible to neutralization or other offset by rivals"); *Innovation Ventures, LLC v. N.V.E., Inc.*, [694 F.3d 723 \(6th Cir. 2012\)](#) (defendant's sending of letter stating that rival committed trademark infringement and false marking and suggesting that retailers sell its product exclusively did not violate the Sherman Act when there was no evidence that the letter caused injury and in any event could easily be rebutted); *Spanish Broad. Sys. of Fla., Inc. v. Clear Channel Commc'ns, Inc.*, [376 F.3d 1065 \(11th Cir. 2004\)](#) (claims that defendant made misrepresentations about the plaintiff, tried to use its leverage in a related market to obtain preferential treatment from auditors and investors, and engaged in a bidding war did not state §2 claim, particularly where the market as a whole and the plaintiff's own sales were expanding during the relevant period); *Taylor Publ'g Co. v. Jostens, Inc.*, [216 F.3d 465 \(5th Cir. 2000\)](#) (dominant firm lured customers with low price offers, but later convinced them to purchase additional items at premium prices; no coercion of customers; no antitrust violation); *American Prof'l Testing Serv., Inc. v. Harcourt, Brace, Jovanovich*, [108 F.3d 1147 \(9th Cir. 1997\)](#) (dominant offeror of bar review courses sent five anonymous and damaging fliers about plaintiff rival to law schools over a two-month period; Ninth Circuit requires proof of a "significant and enduring adverse impact on competition," quoting this Paragraph in previous edition; very little evidence that law students actually relied on the fliers in making their decisions); *Hon Hai Precision Indus. Co., Ltd. v. Molex, Inc.*, [2009 WL 310890, 2009-1 Trade Cas. P76,502 \(N.D. Ill. Feb. 9, 2009\)](#) (patentee did not violate §2 by telling one licensee that certain parts were not covered by the patent, when complaining licensee was producing those parts); *Options Nat'l Fertility Registry v. American Soc'y for Reprod. Med.*, [2009 WL 1393555, 2009-1 Trade Cas. P76,620 \(N.D. Cal. May 15, 2009\)](#) (fertility registry of human egg donors that claimed it was driven from business by defamatory statements made by organization that promoted reproductive medicine and technology failed to show causation; granting leave to amend). By contrast, *National Association of Pharmaceutical Manufacturers, Inc. v. Ayerst Laboratories*, [850 F.2d 904 \(2d Cir. 1988\)](#), held that the plaintiff's claim of monopolization by false statements to buyers should not have been dismissed. A manufacturer of name brand drugs had sent pharmacists a letter warning them of the dangers of certain generic drugs, cautioning against use of the plaintiff's generic product for some conditions. The court concluded that the plaintiff should be allowed discovery on its claim that the letter's assertions were "clearly false, clearly material, and clearly likely to induce reasonable reliance." *Id.* at 916. Of course, these facts alone would not be sufficient to establish the §2 violation; a showing of power and exclusionary effect would also be necessary. See also *Davis v. Southern Bell Tel. & Tel. Co.*, [1994 WL 912242, 1994-1 Trade Cas. P70510 \(S.D. Fla. Feb. 1, 1994\)](#) (telephone company could have monopolized market for inside telephone wire maintenance by using deceptive and coercive marketing tactics that led customers to believe that such services were necessary or economically sensible alternatives to plaintiff's offerings). In *International Travel Arrangers, Inc. v. Western Airlines, Inc.*, [623 F.2d 1255 \(8th Cir.\)](#), cert. denied, [449 U.S. 1063 \(1980\)](#), Western Airlines, which was found to have a monopoly of air carriage from the Twin Cities to Hawaii, placed advertisements discouraging public patronage of certain charters organized by the plaintiff. The special master found the advertisements deceptive in several ways, including a statement that all such charters already scheduled had been canceled and that travel agents understood the pros and cons of such charters. The falsity of the first statement was admitted. The Eighth Circuit found sufficient evidence that the advertisement was false, deceptive, and misleading. *Id.* at 1264. The decline in inquiries, bookings, and requests after the advertisement demonstrated its anticompetitive significance to the court.

deception effectively. Of course, even honest advertising by a dominant firm can deter new entrants, but we virtually always consider honest advertising as competition on the merits.

In *American Council* the Sixth Circuit severely qualified its *Conwood* decision.³⁰ The earlier decision had condemned deceptions made to retailers about their own sales without any inquiry into materiality, reasonable reliance, or even the plausibility that such information could cause significant exclusion of any rival. The latter decision quoted the six requirements listed above, but then added:

[W]e decline to consider each element or hold that all elements must be satisfied to rebut the *de minimis* presumption. We do hold, however, that a plaintiff must show a genuine issue of material fact regarding at least the following two elements to rebut the *de minimis* presumption: (1) the advertising was clearly false, and (2) it would be difficult or costly for the plaintiff to counter the false advertising.

False advertising cannot help consumers, and hence cannot be defended as beneficial to competition. Evidence on the second element is required because even false advertising would not damage competition and hence be a violation of the Sherman Act unless it was so difficult for the plaintiff to counter that it could potentially exclude competition. ... Isolated business torts, such as falsely disparaging another's product, do not typically rise to the level of a section 2 violation unless there is a harm to competition itself.³¹

The court contrasted its *Conwood* decision because in that case the information claimed to be false was part of a broader pattern of activity. But *Conwood* expressly repudiated any need to measure anticompetitive effects and permitted a form of proof that intermixed

³⁰ *American Council of Certified Podiatric Physicians & Surgeons v. American Bd. of Podiatric Surgery*, [323 F.3d 366 \(6th Cir. 2003\)](#). On *Conwood Co., L.P. v. United States Tobacco Co.*, [290 F.3d 768 \(6th Cir. 2002\)](#), cert. denied, **537 U.S. 1198 (2003)**, see 782a2.

³¹ *American Council*, [323 F.3d at 371-72](#), quoting this Paragraph in a previous edition, as well as numerous decisions.

procompetitive, competitively harmless, and anticompetitive conduct with no distinction among their effects.³²

And in *Covad* the D.C. Circuit rejected the plaintiff Internet carrier's claim that Bell Atlantic, the dominant provider of Internet services in the region, misleadingly advertised the availability of its DSL services and exaggerated their scope in order to induce customers away from the service offered by its competitor. Effectively, Bell Atlantic created the impression that it was "ready, willing and capable of providing DSL services" when in fact it was not.³³ Covad then further alleged a "bait and switch." When customers called in to order the DSL service, which in fact was not yet available, Bell Atlantic's representatives tried to turn the customer to its slower ISDN service.³⁴ The court concluded that these

³² See also *Santana Prods., Inc. v. Bobrick Washroom Equip., Inc.*, [401 F.3d 123 \(3d Cir.\)](#), cert. denied, **546 U.S. 1031 (2005)**, in which defendants' alleged representations to government architects who influenced purchasing decisions that plaintiff's products were unsafe were not actionable when the purchasing decisions themselves were made by the government; finding it unnecessary to decide the *Noerr-Pennington* issue-see [P201](#) - P208 -because there was no restraint of trade: We fail ... to find "restraint" in this alleged activity. ... Here, Santana's antitrust claim is built on allegations that the defendants criticized the safety of HDPE partitions. It is undisputed that the defendants informed potential customers that Santana's product presented safety hazards. Santana has not, however, demonstrated that Bobrick imposed any restraints on trade. Santana does not allege that Bobrick engaged in coercive measures that prevented Santana from selling its products to any willing buyer or prevented others from dealing with Santana. Moreover, Santana's allegations of fraud in the manner in which the hazards of HDPE were portrayed are irrelevant because "deception, reprehensible as it is, can be of no consequence so far as the Sherman Act is concerned." *Noerr*, [365 U.S. at 145](#); cf. *Schachar*, [870 F.2d at 399](#) ("antitrust law does not compel your competitor to praise your product or sponsor your work."). [Quoting *Schachar v. American Academy of Ophthalmology, Inc.*, [870 F.2d 397 \(7th Cir. 1989\)](#)]. ...Here, the defendants' marketing campaign was aimed primarily at persuading government architects to specify Bobrick's materials instead of materials made from HDPE. It was the architects who would make the ultimate decision of which product to specify for use in a particular project. This is classic competition on the merits of a product. In no real sense is Santana excluded from the toilet partition market. Santana remains free to tout its product to the specifiers and remains equally free to reassure them that its partitions are superior to Bobrick's partitions and to prove Bobrick wrong with respect to the flammability of HDPE partitions. Toilet partition buyers are in no way constrained from buying HDPE toilet partitions. "The central insight ... is that jockeying over specifications ... is a valid form of competition. ... This behavior was 'simple salesmanship' that enhanced rather than subverted competition on the merits. If ... [Santana] was 'excluded,' it was excluded by ... [Bobrick's] superior product or business acumen." [401 F.3d 132-33](#) (internal citations omitted). On pleading requirements in §2 false information cases, see *Tate v. Pacific Gas & Electric Co.*, [230 F. Supp. 2d 1072, 1080 \(N.D. Cal. 2002\)](#): Plaintiffs have not pled that the defendant's disparaging comments were clearly likely to induce reasonable reliance by the public or private clients, or that disparaging comments were made to buyers without knowledge of the subject matter, or that the violations were not readily susceptible to neutralization or other offsets by rivals.

³³ *Covad Commc'ns Co. v. Bell Atl. Corp.*, [398 F.3d 666, 674 \(D.C. Cir. 2005\)](#). See also *Reed Constr. Data Inc. v. McGraw-Hill Cos.*, [638 Fed. Appx. 43 \(2d Cir. 2016\)](#) (dismissing §2 claim where advertising was not shown to be sufficiently material to influence any customer's decision); *Duty Free Ams., Inc. v. Estée Lauder Co.*, [797 F.3d 1248 \(11th Cir. 2015\)](#) (dismissing complaint of monopolization by dealer disparagement by cosmetic manufacturer because its statements were not shown to be substantially false; defendant Estée Lauder had identified "quality dealers" to airport authorities but did not mention the plaintiff as one of these; it also told them that it had not dealt with the plaintiff; in addition, the evidence showed "robust competition between the duty free operators to obtain airport leases." *Id.* at 1269-70.).

allegations failed to suggest "plausible harm to competition, let alone a case of attempted monopolization." ³⁵ In fact, the court held, the practice increased the amount of competition by presenting customers with the offer of the older ISDN service as an alternative to DSL. ³⁶ The court distinguished other cases involving the defendant's spreading of false information, because in those the falsity was relatively difficult for customers to discover. ³⁷ However,

although Covad does not elaborate, we believe its point is that some potential customers, after attempting to order DSL service from Bell Atlantic only to discover it was unavailable, decided to wait for Bell Atlantic's service to become available rather than immediately patronizing Covad. ...

Here, the alleged falsehood pertains only to whether Bell Atlantic's DSL service was then available. When a company falsely claims or implies its own service is available and the falsity of that claim is necessarily dispelled whenever a consumer tries to obtain the service, there can be no plausible harm to competition; upon discovering the service is not available, the consumer may choose freely whether to purchase the service from another source or to wait for the offeror to make good. ³⁸

Klein v. Facebook, Inc. , 580 F. Supp. 3d 743 (N.D. Cal. 2022) (consumers and advertisers adequately alleged in class action that Meta (Facebook) engaged in monopolistic deception with statements about its data privacy practices that were obviously false and not readily subject to verification or falsification; further, these misrepresentation were sufficient in attracting users to support allegation that they contributed to the creation of FB's dominant market position; citing earlier version of this Paragraph).

³⁴ *Covad* , 398 F.3d at 674.

³⁵ *Ibid.*

³⁶ *Ibid.*

³⁷ Discussing *National Ass'n of Pharm. Mfrs., Inc. v. Ayerst Labs.* , 850 F.2d 904 (2d Cir. 1988).

³⁸ *Covad* , 398 F.3d at 675.

EXHIBIT 9

Privacy Progress | Meta

PRIVACY PROGRESS UPDATE

We have a responsibility to protect people's privacy and give them control to make their own choices.

01. HOW WE DO IT

We have dedicated teams and processes to help us do privacy well because it's important to people and our business.

“We’ve made important progress, but we still have a tremendous amount of work to do. We’re in the early phases of a multi-year and ongoing effort to evolve our culture, our operations and our technical systems to honor people’s privacy.”

- Michel Protti, Chief Privacy Officer for Product

Governance

Our work on privacy is underpinned by our internal governance structures that embed privacy and data-use standards across the company's operations. Externally, independent governance bodies provide oversight over our privacy program and practices.

As we continue to integrate privacy across the company, we're embedding privacy teams within product groups that will deepen the understanding of privacy considerations by providing expertise within each product and business group. These teams enable front-line ownership of privacy responsibilities across our products.

Led by Chief Privacy Officer, Product, Michel Protti, the Meta Privacy and Data Practices team is made up of dozens of teams, both technical and non-technical, focused on privacy and responsible data practices.

The Meta Privacy and Data Practices Team is at the center of our company's efforts to maintain a comprehensive privacy program. Its mission –to instill responsible data practices across Meta– guides this work by ensuring people understand how Meta uses their data and trust that our products

04. ONGOING COMMITMENT TO PRIVACY

We're invested in privacy and are committed to continuous improvement.

“Getting privacy right is a continual, collective investment across our company, and is the responsibility of everyone at Meta to advance our mission.” - Michel Protti, Chief Privacy Officer for Product

Protecting users' data and privacy is essential to our business and our vision for the future. To do so, we're continually refining and improving our privacy program and our products, as we respond to evolving expectations and technological developments – working with policy makers and data protection experts to find solutions to unprecedented challenges – and sharing our progress as we do.

EXHIBIT 10



[Back to Newsroom](#)

[Meta](#)

Introducing Study from Facebook

June 11, 2019



By Sagee Ben-Zedeff, Product Manager

Update on March 23, 2020 at 9:00AM PT: We'll now run Study through [Facebook Viewpoints](#), our market research app, instead of through Applause. This means you'll need a Facebook Viewpoints account to participate in the Study research

program. For more information, download the Study app.

Originally published on June 11, 2019 at 9:00AM PT:

Market research helps companies build better products for people. We believe this work is important to help us improve our products for the people who use Facebook. We also know that this kind of research must be clear about what people are signing up for, how their information will be collected and used, and how to opt out of the research at any time.

Earlier this year, we announced that we'd be shifting our focus to reward-based market research programs, which means that all research participants are compensated. Today we are launching a new market research app called Study from Facebook.

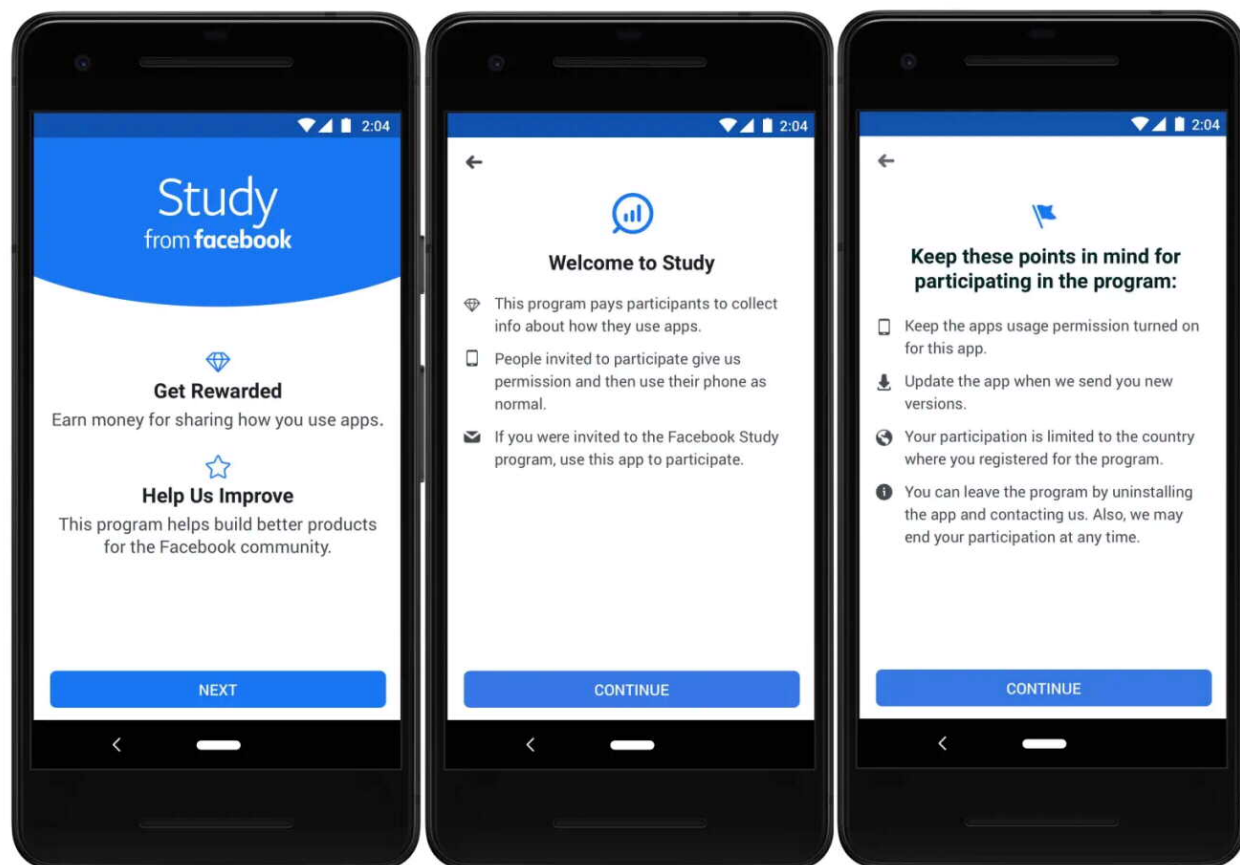
We've learned that what people expect when they sign up to participate in market research has changed, and we've built this app to match those expectations. We're offering transparency, compensating all participants, and keeping people's information safe and secure.

Signing Up to Participate

Here's how it works. We'll run ads to encourage people to participate in this market research program. When someone clicks on an ad, they'll have the option to register and, if they qualify, they'll be invited to download the app. Once invited, they'll find the Study from Facebook app in the Google Play Store. As they sign up, people will see a description of how the app works and what information they'll be sharing with us so they can confirm they want to participate. We also notify users on the Study from Facebook website and in the Play Store description about what information we collect and how it will be used. This is all accessible before participants provide any market research information to the app. Anyone who uses the app will be compensated for contributing to the research. Only people who are 18 and older will be eligible to participate at launch, and all participants will be able to opt out at any time.

To help us manage the logistics of the market research program, we'll work with Applause, a long-time partner who is experienced in managing this type of market

research and works with many other companies in the industry. They'll manage the registration process, all compensation to participants, and customer support.



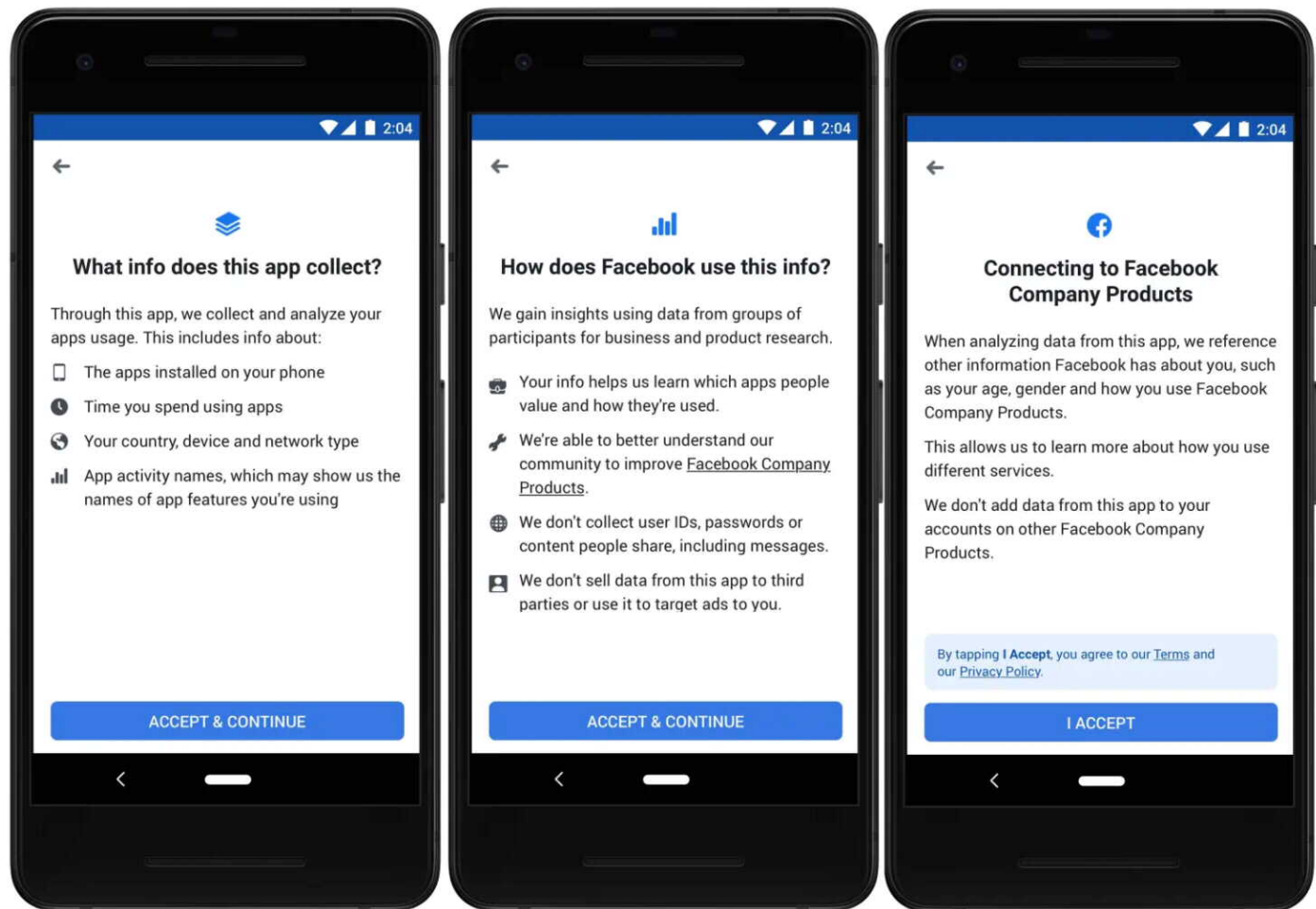
How We Collect Information

We have a responsibility to keep people's information safe and secure. With this app, we're collecting the minimum amount of information needed to help us build better products. People often have a lot of apps on their phone, so we'll periodically remind participants that they are a part of the program. They'll also have the opportunity to review the information they're sharing with us. Through the program, we collect and analyze information including:

- The apps installed on a participant's phone
- The amount of time spent using those apps
- Participant's country, device and network type
- App activity names, which may show us the names of app features participants are using

Study from Facebook does not collect user IDs, passwords, or any of the

participant's content, such as photos, videos, or messages. We also don't sell information from the app to third parties or use it to target ads, and it is not added to a participant's Facebook account if they have one.



At first, the app will only be available to people in the US and India. We'll continue to make it better and expand it to other countries over time.

Approaching market research in a responsible way is really important. Transparency and handling people's information responsibly have guided how we've built Study from Facebook. We plan to take this same approach going forward with other market research projects that help us understand how people use different products and services.

To learn more about the app, visit facebook.com/facebookstudy.

EXHIBIT 11



Here's the transcript of Recode's interview with Facebook CEO Mark Zuckerberg about the Cambridge Analytica controversy and more

"I think we let the community down, and I feel really bad and I'm sorry about that," he said.

By Kara Swisher and Kurt Wagner | Mar 22, 2018, 3:49am EDT



Most Read

- 1 Mental illness is not responsible for America's guns crisis
- 2 When did we get so obsessed with unique baby names?
- 3 Take a mental break with the newest Vox crossword
- 4 Why most car dealers still don't have any electric vehicles
- 5 A frightening virus is killing a massive number of wild birds

Sharing is caring, except this time.

Facebook CEO Mark Zuckerberg gave interviews yesterday to several news organizations, including Recode, in an attempt to stem the fast-growing controversy about misuse of user data by a third-party developer, Cambridge Analytica.

In a wide-ranging interview, he admitted the social networking giant may have made mistakes in opening up its network so much a decade ago and that it led to the recent problems. Zuckerberg said that fixing those issues will now cost the company "many millions" of dollars.

As Facebook's stock continued to get hammered because of Wall Street worries about the impact in its business, Zuckerberg also said he was "open" to testifying to Congress, even as legislators ever more loudly call for his appearance in hearings.

And that is not all Silicon Valley's most famous mogul said, which is why we are posting the transcript of the 20-minute interview, which was conducted by Kara Swisher and Kurt Wagner of Recode.

A short amount of cross-talk about setting up the taping of the interview at the start was removed, but here is the interview (with some small adjustments to explain references made).

Kara Swisher: As you know from us emailing, I'm very interested in tough substantive discussions and questions about this, so that's why I've been so adamant. So let's just get started. Talk a little bit about the things you announced today. Let's have you explain each of them very briefly.

Mark Zuckerberg: Sure. At a high level, this is a major breach of trust issue, and our high-level responsibility is to make sure that this doesn't happen again. So, if you look at the problem, it

V

Future Perfect

Each week, we explore unique solutions to some of the world's biggest problems.

Email (required)

By submitting your email, you agree to our Terms and Privacy Notice. You can opt out at any time. This site is protected by reCAPTCHA and the Google Privacy Policy and Terms of Service apply. For more newsletters, check out our newsletters page.

SUBSCRIBE

Plaintiff Exhibit

Klein et al v Meta Platforms

Mark Zuckerberg

2253

5/9/23, 7:06 AM

Here's the transcript of Recode's interview with Facebook CEO Mark Zuckerberg about the Cambridge Analytica controversy and m...

kind of breaks down into a couple of areas. One is making sure that going forward, developers can't get access to more data than they should. The good news there is that actually the most important changes to the platform we made in 2014, three or four years ago, to restrict apps like [researcher Aleksandr Kogan's] from being able to access a person's "friends" data in addition to theirs.

So that was the most important thing, but then what we did on our platform is we also are closing down a number of other policies. Like, for example, if you haven't used an app in three months, the app will lose the ability to clear your data without you reconfirming it, and a number of things like that. So, that's kind of category 1 going forward. And again, the good news there is that as of three or four years ago, new apps weren't able to do what happened here. So this is largely ... this issue is resolved going forward for a while.

Then there's going backwards, which is before 2014, what are all the apps that got access to more data than people would be comfortable with? And which of them were good actors, like legitimate companies, good intent developers, and which one of them were scams, right? Like, what Aleksandr Kogan was doing, basically using the platform to gather a bunch of information, sell it or share it in some sketchy way. So what we announced there is, we're going to do a full investigation of every single app that had access to a large amount of people's data, before 2014 when we lost out the platform, and if we detect anything suspicious, we're basically going to send in a team to do a full forensic audit, to confirm that no Facebook data is being used in an improper way.

And of course, any developer that isn't comfortable with that, then we'll just ban them from the platform. If we find anything that is bad, then we'll of course also ban the developer, but we will then also notify and tell people, everyone whose data has been affected. Which we're also going to do here.

KS: So that begs the question ... this started off in 2007, 2008 when you were [launching] Facebook Connect, a lot of this stuff started very early, and I remember being at that event where you talked about this. Open and sharing, and it was helpful to growing your platform, obviously. Why wasn't this done before? What's in the mentality of your engineers of Facebook where you didn't suspect this could be a problem?

Well, I don't think it's engineers.

KS: Well, whatever. People [at Facebook].

So, in 2007 we launched the platform.

KS: Yep.

The vision, if you remember is to help make apps social.

KS: Right.

So, the examples we had were, you know, your calendar should have your friend's birthday. Your address book should have your friend's picture. In order to do that, you basically need to make it so a person can log into an app and not just port their own data over, but also be able to bring some data from their friends as well. That was the vision, and a bunch of good stuff got created. There were a bunch of games that people liked. Music experiences, things like Spotify Travel, you know, things like Airbnb they were using it. But there was also a lot of scammy stuff.

There's this values tension playing out between the value of data portability, right? Being able to take your data and some social data ... To be able to create new experiences on the one hand, and privacy on the other hand, and just making sure that everything is as locked down as possible.

You know, frankly, I just got that wrong. I was maybe too idealistic on the side of data portability, that it would create more good experiences. And it created some, but I think what the clear feedback was from our community was that people value privacy a lot more. And they would rather have their data locked down and be sure that nothing bad will ever happen to it than be able to easily take it and have social experiences in other places. So, over time, we have been just kind of narrowing it down. And 2014 was a really big ...

5/9/23, 7:06 AM

Here's the transcript of Recode's interview with Facebook CEO Mark Zuckerberg about the Cambridge Analytica controversy and m...

KS: I get that. 2014 you absolutely did that. But I'm talking about the ... You know — and I've argued with [Facebook executives] about this — this anticipation of problems, of possible bad actors on this platform. Do you all have enough mentality, or do you not see ... I want to understand what happens within Facebook that you don't see that this is so subject to abuse. How do you think about that, and what is your responsibility?

Yeah. Well, I hope we're getting there. I think we remain idealistic, but I think also understand what our responsibility is to protect people now. And I think the reality is is that in the past we had a good enough appreciation of some of this stuff. And some of it was that we were a smaller company, so some of the issues and some of these bad actors just targeted us less, because we were smaller. But we certainly weren't in a target of nation states trying to influence elections back when we only had 100 million people in the community.

But I do think part of this comes from these idealistic values of openness and data portability and things that I think the tech community holds really dear, but are in some conflict with some of these other values, are in protecting people privately, right? And a lot of the most sensitive issues that we faced today are conflicts between our real values, right? Freedom of speech and hate speech and offensive content. Where is the line, right? And the reality is that different people are drawn to different places, we serve people in a lot of countries around the world, a lot of different opinions on that.

KS: Right, so where's your opinion right now? Sorry to interrupt.

On that one specifically?

KS: Yeah.

You know, what I would really like to do is find a way to get our policies set in the way that reflects the values of the community so I'm not the one making those decisions. Right? I feel fundamentally uncomfortable sitting here in California at an office, making content policy decisions for people around the world. So there are going to be things that we never allow, right, like terrorist recruitment and ... We do, I think, in terms of the different issues that come up, a relatively very good job on making sure that terrorist content is off the platform. But things like where is the line on hate speech? I mean, who chose me to be the person that ...

KS: Well. Okay ...

I have to, because [I lead Facebook], but I'd rather not.

KS: I'm going to push back on that, because values are what we argue about. And companies have values, and they have, you know, the New York Times has a set of values that they won't cross and they make decisions. Why are you so uncomfortable making those value decisions? You run the platform. It is more than just a benign platform that is neutral. It just isn't. I don't know, we can disagree on that, we obviously disagree on this. But why are you uncomfortable doing that?

Well, I just want to make the decisions as well as possible, and I think that there is likely a better process, which I haven't figured out yet. So, for now, it's my job, right? And I am responsible for it. But I just wish that there were a way ... a process where we could more accurately reflect the values of the community in different places. And then in the community standards, have that be more dynamic in different places. But I haven't figured it out yet. So I'm just giving this as an example of attention that we debate internally, but clearly until we come up with a reasonable way to do that, that is our job, and I do well in that.

Kurt Wagner: Hey, Mark, this is Kurt. I'm curious, you talked about going back and trying to figure out if there were other developers that had used your API before 2014, and checking were there any other bad actors that maybe you guys missed at the time. I'm curious how you actually go about doing that, and if it's actually possible at this point to go out and detect, you know, if someone collected data in 2012, if that data still exists.

Well, the short answer is the data isn't on our servers so it would require us sending out forensic auditors to different apps. The basic process that we've worked out — and this is a lot of what we were trying to figure out over the last couple of days and why it took a little while to



5/9/23, 7:06 AM

Here's the transcript of Recode's interview with Facebook CEO Mark Zuckerberg about the Cambridge Analytica controversy and m...

get this post out — is we do know all the apps that registered for Facebook and all the people who are on Facebook who register for those apps and have a log of the different data requests that the developer has made.

So we can get a sense of what are reputable companies, what are companies that were doing unusual things ... Like, that either requested data in spurts, or requested more data than it seemed like they needed to have. And anyone who either has a ton of data or something unusual, we're going to take the next step of having them go through an audit. And that is not a process that we can control, they will have to sign up for it. But we'll send in teams, who will go through their servers and just see how they're handling data. If they still have access to data that they're not supposed to, then we'll shut them down and notify ... and tell everyone whose data was affected.

This is a complex process. It's not going to be overnight. It's going to be expensive for us to run, and it's going to take a while. But look, given the situation here, that we had a developer that signed a legal certification saying that they deleted the data, now two years later we're back here and it seems like they didn't, what choice do we have? This is our responsibility to our community is to make sure that we go out and do this. So, even though it's going to be hard and not something that our engineers can just do sitting in their offices here, I still think we have to go do this.

KW: Did you ever think of doing these kinds of audits before 2014? Or even when you got that signed contract from ... or, excuse me, signed statement I guess, from Cambridge Analytica, did you think, "Well, we need to actually go out and check to make sure that they're telling us the truth." Why didn't you do this kind of stuff earlier, or did you think about doing this earlier?

In retrospect, it was clearly a mistake. Right? The basic chronology here is in 2015, a journalist from the Guardian pointed out to us that it seemed like the developer Aleksandr Kogan had sold shared data to Cambridge Analytica and a few other firms. So as soon as we learned that, we took down the app, and we demanded that Kogan, Cambridge Analytica and all the other folks give up the formal, legal certification that they didn't have any other data. And, at the time, Cambridge Analytica told us that not only do we not have the data and it's deleted, but so we actually never got access to raw Facebook data. Right? What they said was, this app that Kogan built, it was a personality quiz app, and instead of raw data they got access to some derived data, some personality scores for people. And they said that they used it in some models and it ended up not being useful so they just got rid of it.

So, given that, that they said that they never had the data and deleted what derivative data that they had, at the time it didn't seem like we needed to go further on that. But look, in retrospect it was clearly a mistake. I'm explaining to you the situation at the time and the actions that we took, but I'm not trying to say it was the right thing to do. I think given what we know now, we clearly should have followed up, and we're never going to make that mistake again.

I think we let the community down, and I feel really bad and I'm sorry about that. So that's why we're going to go and do these broad audits.

KS: All right, when you think about that idea of ... it's not exactly a "mistakes were made" kind of argument, but you are kind of making that. That idea. I want to understand, what systems are going to be in place, but it's sort of, you know, the horses are out of the barn door. Can you actually go get that data from them? Are you ... It's everywhere, I would assume. I've been told by many, many people that have access to your data, I was thinking of companies like RockYou and all kinds of things from a million years ago that have a lot of your data ... Can you actually get it back? I don't think you can. I can't imagine you can.

Not always. But the goal isn't to get the data back from RockYou. You know, people gave their data to RockYou. So RockYou has the right to have the data. What RockYou does not have the right to do is share the data or sell it to someone without people's consent. And part of the audits and what we're going to do is see whether those business practices were in place, and if so we can kind of follow that trail and make sure that developers who might be downstream of that comply or they're going to get banned from our platform overall.

5/9/23, 7:06 AM

Here's the transcript of Recode's interview with Facebook CEO Mark Zuckerberg about the Cambridge Analytica controversy and m...

It isn't perfect. But I do think that this is going to be a major deterrent going backwards. I think it will clean up a lot of data, and going forward the more important thing is just preventing this from happening in the first place, and that's going to be solved by restricting the amount of data that developers can have access to. So I feel more confident that that's going to work, starting in 2014 and going forward. Again, for the last few years already it hasn't been possible for developers to get access to that much.

KS: Let me ask just two more quick questions.

[Here, there is logistical cross-talk with a person on his staff, since Zuckerberg had to head to an employee meeting.]

All right, I'm talking to you while walking over there for Q&A.

KS: All right, the cost of this? And are you going to testify in front of Congress? And if so, when?

You know, I'm open to doing that. I think that the way that we look at testifying in front of Congress is that ... We actually do this fairly regularly, right? There are high-profile ones like the Russian investigation, but there are lots of different topics that Congress needs and wants to know about. And the way that we approach it is that our responsibility is to make sure that they have access to all the information that they need to have. So I'm open to doing it.

KS: What is "open"? Is that a "yes" or a "no"?

Well.

KS: They want you, Mark.

Well look, I am not 100 percent sure that's right. But the point of congressional testimony is to make sure that Congress gets the data in the information context that they need. Typically, there is someone at Facebook whose full-time job is going to be focused on whatever the area is. Whether it's legal compliance, or security. So I think most of the time if what they're really focused on is getting access to the person who is going to be most knowledgeable on that thing, there will be someone better. But I'm sure that someday, there will be a topic that I am the person who has the most knowledge on it, and I would be happy to do it then.

KW: Mark, can you give us a sense of the timing and cost for this? Like, the audits that you're talking about. Is there any sense of how quickly you could do it and what kind of cost it would be to the company?

I think it depends on what we find. But we're going to be investigating and reviewing tens of thousands of apps from before 2014, and assuming that there's some suspicious activity we're probably going to be doing a number of formal audits, so I think this is going to be pretty expensive. You know, the conversations we have been having internally on this is, "Are there enough people who are trained auditors in the world to do the number of audits that we're going to need quickly?" But I think this is going to cost many millions of dollars and take a number of months and hopefully not longer than that in order to get this fully complete.

KS: Okay, last question Mark, and then you can go. How badly do you think Facebook has been hurt by this, and you yourself, the reputation of Facebook?

I think it's been a pretty big deal. The No. 1 thing that people care about is privacy and the handling of their data. You know, if you think about it, the most fundamental thing that our services are, whether it's Facebook or Whatsapp or Instagram, is this question of, "Can I put content into it?" Right? Whether it's a photo or a video or a text message. And will that go to the people I want to send it to and only those people? And whenever there is a breach of that, that undermines the fundamental point of these services. So I think it's a pretty big deal, and that's why we're trying to make sure we fully understand what's going on, and make sure that this doesn't happen again. I'm sure there will be different mistakes in the future, but let's not make this one again.

KS: Yes, let's not. Okay, Mark, I really appreciate you talking to us.

5/9/23, 7:06 AM Here's the transcript of Recode's interview with Facebook CEO Mark Zuckerberg about the Cambridge Analytica controversy and m...

KW: Okay, Mark.

KS: Thank you so much, I know you have to talk to your employees ...

I'm walking into my Q&A now. All right, see ya.

This article originally appeared on Recode.net.

You've read 2 articles in the last 30 days.

Will you help keep Vox free for all?

At Vox, we believe that clarity is power, and that power shouldn't only be available to those who can afford to pay for a subscription. That's why we keep our work free. Millions rely on Vox's clear, high-quality journalism to understand the forces shaping today's world. **Support our mission and help keep Vox free for all by making a financial contribution to Vox today.**

One-TimeMonthlyAnnual

☐ \$95/year

☒ **\$120/year**

☐ \$250/year

☐ \$350/year

☐ Other

Yes, I'll give \$120/year

We accept credit card, Apple Pay, and Google Pay. You can also contribute via




EXHIBIT 12



EXHIBIT 6

9.17.2018

App Developer Investigation & Enforcement

September 2018 Status and Re-scoped Approach



ADI Timeline to Date

March 2018 – April 2018

- March 21: Mark committed to investigate and audit all suspicious v1 apps
 - “We will **investigate all apps** that had access to **large amounts of information** before we changed our platform to dramatically reduce data access in 2014, and we will conduct a **full audit of any app with suspicious activity.**”
- April 5-6: Final decisioning regarding which outside consultants to engage
- April 6: **Phase I** kick-off; DevOps prioritization of initial review through App Litigation Tool (“ALT”)
 - Prioritized by buckets (P0, P1, and P2) across multiple APIs
 - P0 Platform started with ~3200 apps, overall v1 prioritization currently covers **11 million apps**
 - ALT reviewers staffed through DevOps (from a group of 60, rotating team of 30-40 reviewers)
- April 9: **Phase II** kick-off (in advance of Mark’s April 10 testimony); engaging of Stroz Friedberg and FTI Consulting as ADI investigators, under direction of GDC
- April 23: First wave of ADI investigators and attorneys provisioned
- April 26: ADI investigators begin background investigations and initial reports for review, feedback, and refinement

ADI Status – Hi-Pri Escalations

As of September 17, 2018

- ADI and GDC have handled 30+ hi-pri escalations to date
- Hi-pri escalations typically arise from a source other than the ALT/ADI workflow, e.g., internal Facebook reporting, media reports, or political interest
- Gibson Dunn, FTI, and Stroz work up the app in around 48-72 hours, although some investigations take around a week
- The full work-up may include: a background investigation/report, a technical investigation/report, a factual summary and analysis, an analysis of potential policy and legal violations, developed recommendations on next steps, comms consultations, regulatory response consultations, and (if the developer has counsel) communications with counsel
- The list below represents escalations handled in roughly the last 3.5 months, since mid-May 2018

Profile Technology / Profile Engine	Fast Likers Developers	QuizzStar	GupShup	Crimson Hexagon
CubeYou/CPC / You Are What You Like	myPersonality data takedowns (GitHub, Tableau, Kaggle, RapidMiner, Google)	Social Video Downloader	Meltwater / Connect	Spredfast
CPC/Stillwell/Kosinski / myPersonality	Social Sweethearts	Zubizu	Branch.io	Sysomos apps
CPC/Stillwell / Apply Magic Sauce	VonVon	Censia	Mail.ru	
Guard.Social / Social Pain Killer	Sync Me	Moves Platform	TrolleyBust	
Project Peoria	Becklicka	AIQ / WPA	TimeHop	
CPC/myDays	Social Data Hub	Lovoo/Voo	Walrus Music	

PRIVILEGED & CONFIDENTIAL – ATTORNEY-CLIENT COMMUNICATION – FOR INTERNAL USE ONLY – DO NOT DISTRIBUTE

ADI Goals & Approach – Revised

- **Risk-based prioritization of other pre-2014-platform-changes apps for ADI review (cont.)**
 - **High-Risk Countries**
 - **Goal:** Review apps of developers located in certain “high-risk” jurisdictions, because those jurisdictions may be governed by potentially risky data storage and disclosure rules or be more likely to house malicious actors
 - **Status:** Under development
 - We ran preliminary queries on a test set of 9 suggested countries to understand the number of developers in those jurisdictions and review any facially interesting results—see next slide for numbers of developers
 - E.g., some countries have a relatively small number of developers that created pre-2014 apps; Iran had a significant number of seemingly Russian developers
 - Based on a review of lists prepared by government agencies (e.g., State Dept., FBI, OFAC) and watchdog organizations (e.g., FireEye), we have now identified 28 countries for our review, and elaborated the rationale for including those countries
 - E.g., states known to collect data for intelligence targeting and cyber espionage
 - We will separately review China and Russia, given the risk associated with those countries
 - For other jurisdictions, we have identified them as tier 1 and tier 2 risk to assist in prioritizing
 - We are in the process of identifying the total number of developers in each country, and will take into account learnings from other categories to prioritize our review of this category

ADI Goals & Approach – Revised

- Risk-based prioritization of other pre-2014-platform-changes apps for ADI review (cont.)
 - *High-Risk Countries*

Developers in Test Set of High-Risk Jurisdictions	
Summary of Developers by Predicted Country	
Country	# of Developers
China	86,961
Cuba	250
Iran	2,533
North Korea	21
Russia	42,078
Sudan	647
Syria	929
Ukraine	34,624
Vietnam	76,813
* Country determination is based on the country field in the dim_all_users_sensitive:bi table. * Only includes developers of apps with over 10 installed users. Excludes developers and apps identified as Facebook internal.	

ADI Team & Pace

Where We Are Today

- **ALT** has reviewed 0.1% of the 11 million apps and objects that DevOps has identified for ADI review (11,435 as of August 8)
 - ALT has escalated approximately 20% of apps it reviews (2,373 as of August 8)
- **Stroz Friedberg and FTI Consulting** have over 60 and over 130 consultants working on ADI, respectively
 - Combined, they are producing about 150 background reports on escalated apps per week (total of 1,238 as of August 8)
 - Stroz and FTI each have personnel onsite, which facilitates speedy interaction with multiple Facebook groups
 - Stroz, FTI, and GDC, are constantly ready, and regularly called upon, to assist with high priority and other escalations
- **Gibson Dunn** has attorneys onsite daily, overseeing ADI and ready to handle rapid response escalations; there are often as many as 5 hi-pri diversions a day
- **Looking Ahead**
 - Given the number of apps, our original estimate was that the current structure would operate through at least 2020
 - Having now completed about four months of review this work, we have a better understanding of the process and risk
 - **Now is an opportunity to reflect and consider alternative approaches to better risk-calibrate the investigation**

EXHIBIT 13

MARK R. WARNER, VIRGINIA, CHAIRMAN
MARCO RUBIO, FLORIDA, VICE CHAIRMAN

DIANNE FEINSTEIN, CALIFORNIA
RON WYDEN, OREGON
MARTIN HEINRICH, NEW MEXICO
ANGUS S. KING, JR., MAINE
MICHAEL F. BENNET, COLORADO
ROBERT P. CASEY, JR., PENNSYLVANIA
KIRSTEN GILLIBRAND, NEW YORK

RICHARD BURR, NORTH CAROLINA
JAMES E. RISCH, IDAHO
SUSAN M. COLLINS, MAINE
ROY BLUNT, MISSOURI
TOM COTTON, ARKANSAS
JOHN CORNYN, TEXAS
BEN SASSE, NEBRASKA

United States Senate

SELECT COMMITTEE ON INTELLIGENCE

WASHINGTON, DC 20510-6475

CHARLES SCHUMER, NEW YORK, EX OFFICIO
MITCH MCCONNELL, KENTUCKY, EX OFFICIO
JACK REED, RHODE ISLAND, EX OFFICIO
JAMES M. INHOFE, OKLAHOMA, EX OFFICIO

MICHAEL CASEY, STAFF DIRECTOR
BRIAN W. WALSH, MINORITY STAFF DIRECTOR
KELSEY S. BAILEY, CHIEF CLERK

Exhibit

Klein, et al v. Meta Platforms Inc

Stacy Chen

2439

February 6, 2023

Mark Zuckerberg
Chief Executive Officer, Meta Platforms Inc.
1 Hacker Way
Menlo Park, CA 94025

Dear Mr. Zuckerberg:

We write you with regard to recently unsealed documents in connection with pending litigation your company, Meta, is engaged in. It appears from these documents that Facebook has known, since at least September 2018, that hundreds of thousands of developers in countries Facebook characterized as “high-risk,” including the People’s Republic of China (PRC), had access to significant amounts of sensitive user data. As leaders of the Senate Intelligence Committee, we write today with a number of questions regarding these documents and the extent to which developers in these countries were granted access to American user data.

In 2018, the *New York Times* revealed that Facebook had provided privileged access to key application programming interfaces (APIs) to Huawei, OPPO, TCL, and other device-makers based in the PRC.¹ Under the terms of agreements with Facebook dating back to at least 2010, these device manufacturers were permitted to access a wealth of information on Facebook’s users, including profile data, user IDs, photos, as well as contact information and even private messages.² In the wake of these revelations, as well as broader revelations concerning Facebook’s lax data security policies related to third-party applications, our staffs held numerous meetings with representatives from your company, including with senior executives, to discuss who had access to this data and what controls Facebook was putting in place to protect user data in the future.

¹ Michael LaForgia and Gabriel J.X. Dance, “Facebook Gave Data Access to Chinese Firms Flagged by U.S. Intelligence,” *New York Times* (June 5, 2018), available at <https://www.nytimes.com/2018/06/05/technology/facebook-device-partnerships-china.html>

² Gabriel J.X. Dance, Nicholas Confessore, and Michael LaForgia, “Facebook Gave Device Makers Deep Access to Data on Users and Friends,” *New York times* (June 3, 2018), available at <https://www.nytimes.com/interactive/2018/06/03/technology/facebook-device-partners-users-friends-data.html>

Given those discussions, we were startled to learn recently, as a result of this ongoing litigation and discovery, that Facebook had concluded that a much wider range of foreign-based developers, in addition to the PRC-based device-makers, also had access to this data. According to at least one internal document, this included nearly 90,000 separate developers in the People's Republic of China (PRC), which is especially remarkable given that Facebook has never been permitted to operate in the PRC.³ The document also refers to discovery of more than 42,000 developers in Russia, and thousands of developers in other "high-risk jurisdictions," including Iran and North Korea, that had access to this user information.

As Facebook's own internal materials note, those jurisdictions "may be governed by potentially risky data storage and disclosure rules or be more likely to house malicious actors," including "states known to collect data for intelligence targeting and cyber espionage."⁴ As the Chairman and Vice Chairman of the Senate Select Committee on Intelligence, we have grave concerns about the extent to which this access could have enabled foreign intelligence service activity, ranging from foreign malign influence to targeting and counter-intelligence activity.

In light of these revelations, we request answers to the following questions on the findings of Facebook's internal investigation:

- 1) The unsealed document notes that Facebook conducted separate reviews on developers based in the PRC and Russia "given the risk associated with those countries."
 - What additional reviews were conducted on these developers?
 - When was this additional review completed and what were the primary conclusions?
 - What percentage of the developers located in the PRC and Russia was Facebook able to definitively identify?
 - What communications, if any, has Facebook had with these developers since its initial identification?
 - What criteria does Facebook use to evaluate the "risk associated with" operation in the PRC and Russia?
- 2) For the developers identified as being located within the PRC and Russia, please provide a full list of the types of information to which these developers had access, as well as the timeframes associated with such access.

³ Exhibit 6, "App Developer Investigation & Enforcement: September 2018 Status and Re-Scoped Approach," Facebook (September 17, 2018), available at <https://storage.courtlistener.com/recap/gov.uscourts.cand.327471/gov.uscourts.cand.327471.1100.6.pdf>

⁴ Exhibit 6, "App Developer Investigation & Enforcement: September 2018 Status and Re-Scoped Approach," Facebook (September 17, 2018), available at <https://storage.courtlistener.com/recap/gov.uscourts.cand.327471/gov.uscourts.cand.327471.1100.6.pdf>

- 3) Does Facebook have comprehensive logs on the frequency with which developers from high-risk jurisdictions accessed its APIs and the forms of data accessed?
- 4) Please provide an estimate of the number of discrete Facebook users in the United States whose data was shared with a developer located in the each country identified as a “high-risk jurisdiction” (broken out by country).
- 5) The internal document indicates that Facebook would establish a framework to identify the “developers and apps determined to be most potentially risky[.]”
 - How did Facebook establish this rubric?
 - How many developers and apps based in the PRC and Russia met this threshold? How many developers and apps in other high-risk jurisdictions met this threshold?
 - What were the specific characteristics of these developers that gave rise to this determination?
 - Did Facebook identify any developers as too risky to safely operate with? If so, which?
- 6) The internal document references your public commitment to “conduct a full audit of any app with suspicious activity.”
 - How does Facebook characterize “suspicious activity” and how many apps triggered this full audit process?
- 7) Does Facebook have any indication that any developers’ access enabled coordinated inauthentic activity, targeting activity, or any other malign behavior by foreign governments?
- 8) Does Facebook have any indication that developers’ access enabled malicious advertising or other fraudulent activity by foreign actors, as revealed in public reporting?⁵

Thank you for your prompt attention.

Sincerely,



Mark R. Warner
Chairman



Marco Rubio
Vice Chairman

⁵ Craig Silverman and Ryan Mac, “Facebook Profits as Users Are Ripped Off by Scam Ads,” (December 10, 2020), available at <https://www.buzzfeednews.com/article/craigsilverman/facebook-ad-scams-revenue-china-tiktok-vietnam>

EXHIBIT 14

An Update on Our Plans to Restrict Data Access on Facebook | Meta

By [Mike Schroepfer](#), Chief Technology Officer

Two weeks ago we promised to take a hard look at the information apps can use when you connect them to Facebook as well as other data practices. Today, we want to update you on the changes we're making to better protect your Facebook information. We expect to make more changes over the coming months — and will keep you updated on our progress. Here are the details of the nine most important changes we are making.

Events API: Until today, people could grant an app permission to get information about events they host or attend, including private events. This made it easy to add Facebook Events to calendar, ticketing or other apps. But Facebook Events have information about other people's attendance as well as posts on the event wall, so it's important that we ensure apps use their access appropriately. Starting today, apps using the API will no longer be able to access the guest list or posts on the event wall. And in the future, only apps we approve that agree to strict requirements will be allowed to use the Events API.

Groups API: Currently apps need the permission of a group admin or member to access group content for closed groups, and the permission of an admin for secret groups. These apps help admins do things like easily post and respond to content in their groups. However, there is information about people and conversations in groups that we want to make sure is better protected. Going forward, all third-party apps using the Groups API will need approval from Facebook and an admin to ensure they benefit the group. Apps will no longer be able to access the member list of a group. Apps can see all posts and comments in the group, but they can't see a group member's name, profile picture or that the group member is the author of posts and comments unless the member allows access. **(Updated on March 2, 2022 at 12:00PM PT to clarify what information apps can see.)**

Pages API: Until today, any app could use the Pages API to read posts or comments from any Page. This let developers create tools for Page owners to help them do things like schedule posts and reply to comments or messages. But it also let apps access more data than necessary. We want to make sure Page information is only available to apps providing useful services to our community. So starting today, all future access to the Pages API will need to be approved by Facebook.

Facebook Login: Two weeks ago we announced [important changes](#) to Facebook Login. Starting today, Facebook will need to approve all apps that request access to information such as check-ins, likes, photos, posts, videos, events and groups. We started approving these permissions in 2014, but

now we're tightening our review process — requiring these apps to agree to strict requirements before they can access this data. We will also no longer allow apps to ask for access to personal information such as religious or political views, relationship status and details, custom friends lists, education and work history, fitness activity, book reading activity, music listening activity, news reading, video watch activity, and games activity. In the next week, we will remove a developer's ability to request data people shared with them if it appears they have not used the app in the last 3 months.

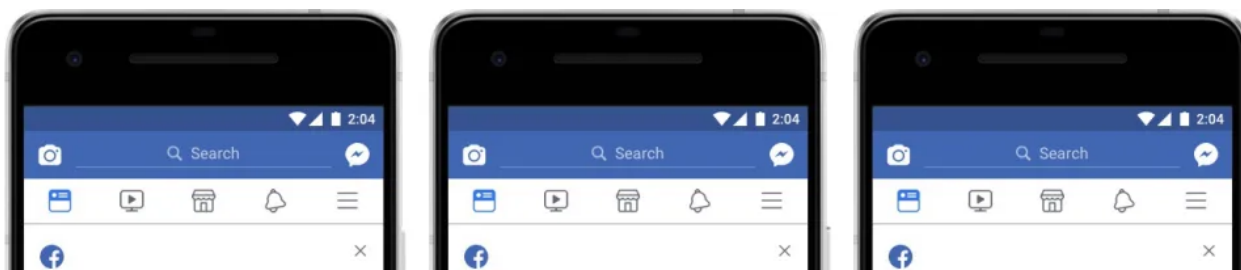
Instagram Platform API: We're making the recently announced deprecation of the Instagram Platform API effective today. You can find more information [here](#).

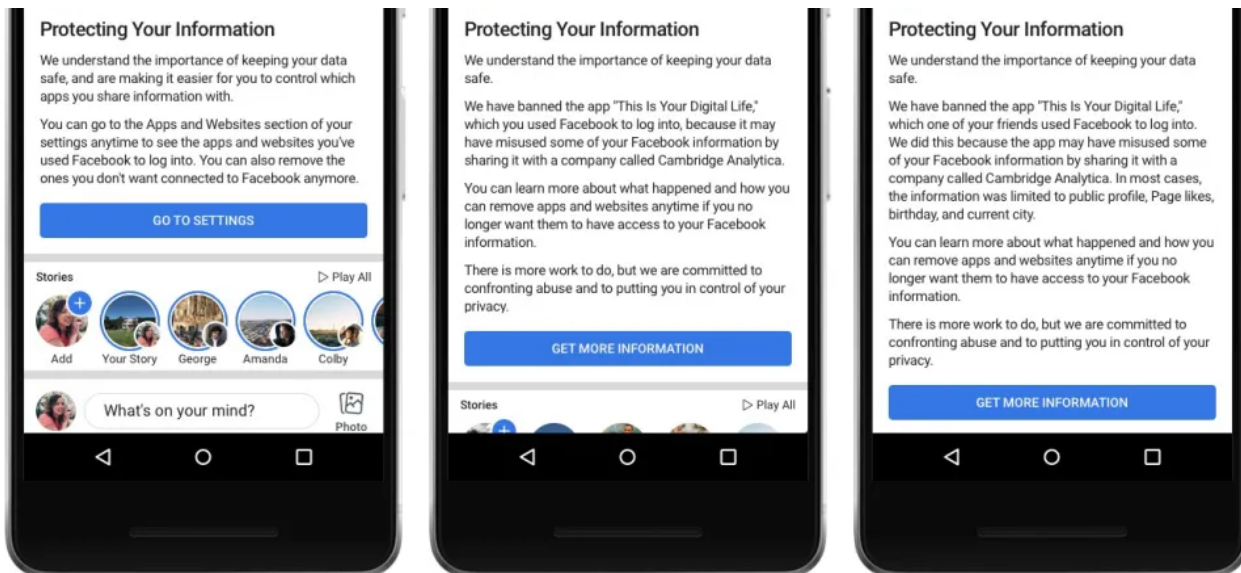
Search and Account Recovery: Until today, people could enter another person's phone number or email address into Facebook search to help find them. This has been especially useful for finding your friends in languages which take more effort to type out a full name, or where many people have the same name. In Bangladesh, for example, this feature makes up 7% of all searches. However, malicious actors have also abused these features to scrape public profile information by submitting phone numbers or email addresses they already have through search and account recovery. Given the scale and sophistication of the activity we've seen, we believe most people on Facebook could have had their public profile scraped in this way. So we have now disabled this feature. We're also making changes to account recovery to reduce the risk of scraping as well.

Call and Text History: Call and text history is part of an opt-in feature for people using Messenger or Facebook Lite on Android. This means we can surface the people you most frequently connect with at the top of your contact list. We've reviewed this feature to confirm that Facebook does not collect the content of messages — and will delete all logs older than one year. In the future, the client will only upload to our servers the information needed to offer this feature — not broader data such as the time of calls.

Data Providers and Partner Categories: Last week we [announced](#) our plans to shut down Partner Categories, a product that lets third-party data providers offer their targeting directly on Facebook.

App Controls: Finally, starting on Monday, April 9, we'll show people a link at the top of their News Feed so they can see what apps they use — and the information they have shared with those apps. People will also be able to remove apps that they no longer want. **As part of this process we will also [tell people](#) if their information may have been improperly shared with [Cambridge Analytica](#).**





Updated April 9, 2018: Three versions of the messages we're sending to people based on whether they've been affected by the app "This Is Your Digital Life." These messages link to facebook.com/help/yourinfo.

In total, we believe the Facebook information of up to 87 million people — mostly in the US — may have been improperly shared with Cambridge Analytica.



(Update on May 1, 2018: Click [here](#) to see a state-by-state breakdown in the US of people whose Facebook information may have been improperly shared with Cambridge Analytica.)

Overall, we believe these changes will better protect people's information while still enabling

developers to create useful experiences. We know we have more work to do — and we'll keep you updated as we make more changes. You can find more details on the platform changes in our [Facebook Developer Blog](#).

EXHIBIT 15

facebook

Email

Keep me logged in

Password

Forgot your password?

Login

Sign Up

Facebook helps you connect and share with the people in your life.

The Facebook Blog

- Facebook Page
- Subscribe to RSS Feed

A New Suite of Safety Tools
by Arturo Bejar on Tuesday, April 19, 2011 at 4:46am

Safety has always been a social experience: as friends and family, we look out for each other and pass along advice to help each other stay safe. Safety on Facebook works the same way. By keeping each other informed, people make Facebook a more trusted environment. Today, we're making it easier to stay safe with the launch of new safety resources, tools for reporting issues and additional security features.

More Resources for Families

During President Obama's [White House Conference on Bullying Prevention](#) last month, we announced plans to expand our existing safety resources with new content for families. Beginning today, you can visit the newly redesigned [Family Safety Center](#). There, you'll find useful articles for parents and teens and videos on safety and privacy, as well as many other resources. In the coming weeks, we'll also be providing a free, downloadable guide for teachers, written by safety experts Linda Fogg Phillips, B.J. Fogg and Derek Baird. We hope this guide will help educators with social media in the classroom.

Meet some of the team who work on safety at Facebook, many of whom are also parents.

wrong :(

Ruffle failed to load the Flash SWF file.

Access to fetch has likely been blocked by CORS policy.

If you are the server administrator, please consult the Ruffle wiki for help.

Social Reporting Tools

We also recently unveiled a new [social reporting tool](#) that allows people to notify a member of their community, in addition to Facebook, when they see something they don't like. Safety and child psychology experts tell us that online issues are frequently a reflection of what is happening offline. By encouraging people to seek help from friends, we hope that many of these situations can be resolved face to face. The impact has been encouraging, and we're now expanding social reporting to other major sections of Facebook, including Profiles, Pages and Groups.

Advanced Security Features

We're also starting to introduce Two Factor Authentication, a new feature to help prevent unauthorized access to your account. If you turn this new feature on, we'll ask you to enter a code anytime you try to log into Facebook from a new device. This additional security helps confirm that it's really you trying to log in.

We announced earlier this year that people could experience Facebook over a secure connection using [HTTPS](#). This feature helps protect your personal information and is particularly useful if you're uncertain about the security of your network or you're using public wifi to access Facebook. Today, we're improving HTTPS so if you start using a non-HTTPS application on Facebook, we automatically switch your session back to HTTPS when you're finished.

We think that social solutions to safety will become increasingly important to using the web. Tools like social reporting will help make our community even stronger, and we encourage you to use them.

Arturo, a director of engineering at Facebook, is excited about social reporting.

Like

Sign Up to see what your friends like.

224 comments

Add a comment

Lee Clayton · Baysgarth School
Https should be set to default, because not many people know about it!

243

Like

Reply

April 19 at 4:52am

Lee Clayton · Baysgarth School

Facebook social plugin

Search Blog

Most Popular Stories

The Wisdom of Friends (and Others Too)

14574

9325

More Beautiful Photos

16372

6454

The Role of Advertising on Facebook

5806

 3994

A New Suite of Safety Tools

 560
 378

A Better Mobile Experience

 15666
 4912

Facebook Page

Facebook

 38,045,705

Facebook Favorites

- [Help Center](#)
- [Facebook Security](#)
- [Facebook Developers Blog](#)
- [Facebook Engineering](#)
- [Facebook Ads](#)
- [Facebook Marketing Solutions](#)

Comment Policy

We love your feedback, but be respectful and stay on topic. We reserve the right to delete profane, harassing, abusive and spam comments and to block repeat offenders. [Read more.](#)

Blog Archive

Looking for a specific post? Visit [our full archive](#) of blog posts sorted by categories and dates.

EXHIBIT 16

Mark Zuckerberg Makes Facebook Privacy Sound So Easy

Brian Barrett

Mark Zuckerberg appeared before Congress Tuesday, and for five hours, senators who [appeared to have halting grasp](#) of the company's intricacies questioned the Facebook CEO on topics ranging from Russia to artificial intelligence. **Zuckerberg for the most part gave considered answers to their questions—except when it came to the specifics of [how users can control their privacy](#).**

That Zuckerberg would dodge uncomfortable questions is a disappointment, though maybe no surprise. But when it came to addressing how the company collects and handles data—and what tools it gives you to control that flow of information—Zuckerberg landed repeatedly on a common refrain: Users have complete control over how their data gets used. “This is the most important principle for Facebook: Every piece of content that you share on Facebook, you own and you have complete control over who sees it, and how you share it, and you can remove it at any time,” said Zuckerberg.

But in trying to present this as exculpatory, Zuckerberg misses the point. Offering tools to someone doesn't help at all if they're hard to find, and even harder to understand.

Zuckerberg cited the “inline” controls that Facebook has gifted its users multiple times. What he's referring to specifically seems to be the dropdown menu that you see before you post to Facebook, the one that says **Who should see this?**, and lets you whittle down your audience by friend groups, geography, or not at all.

Which, sure. That helps. But it's also not what's at issue here. The creeping concern around Facebook—and Google and other ad-driven platforms—isn't whether former coworkers can see your current happy hour pics. It's whether an infinite, invisible web of advertisers, marketers, and app developers can. There's no inline control for that, no option before you post not to share your political screed or baby videos with Dove body wash, or some contact lens start-up.

For that, you need to dig deep into Facebook's settings, a click-intensive process full of unclear language and uncertain paths. Here's a [story](#) that walks you through it; it's well over 2,000 words long. And that's the condensed version.

"Based on today's hearing, even Facebook must acknowledge they need to do much more to communicate to users how their platform works, what data they collect on Facebook and off, and how that information is used for advertising," says Joe Jerome, policy analyst at the Center for Democracy & Technology. "Mr. Zuckerberg argued that Facebook needs to provide controls where users are,

when they're posting photos and messaging friends, but global privacy controls have always been a challenge for Facebook—and any social media platform."

To be honest, all you really need to know about Facebook's attitude toward what you share with apps and ad networks is that the social media company doesn't put controls for either under its **Privacy** category. For years, to see which developers might have your information, you've had to go to **Apps and Websites**. To see what advertisers know and see, you have to visit **Ads**, and decipher inscrutable language like "**Can you see online interest-based ads from Facebook?**", which you'll find under **Ads based on your use of websites and apps**.

Are these the controls that Zuckerberg thinks give users complete power over their data? It beggars belief, if so. They're hidden, they're opaque, and they don't do enough to communicate what information, precisely, those third parties have about you and what they do with it. And if you have installer's remorse and want to reclaim your data? Facebook can't help you with that. You need to contact the developer directly, and hope they listen.

To make matters worse, even Facebook doesn't necessarily know what happens to your data after an app accesses it. While questioning Zuckerberg, Senator Richard Blumenthal noted that the personality quiz app that exposed [up to 87 million people's data to political firm Cambridge Analytica](#) clearly stated in its terms of service that the data it collected could be sold. If Facebook can't bother to read all the way through an app's Terms of Service, how can it expect you to read through its own? (And in fact, Zuckerberg acknowledged that most Facebook users likely don't.) **Until October 2015, Facebook even allowed apps to request [access to user inboxes](#), which meant developers could read any message those people sent or received.**

"Going forward, we're going to take a more proactive position on this, and do much more regular stock checks and other reviews of apps, as well as increasing the amount of audits that we do," Zuckerberg said Tuesday. But privacy advocates argue that any added rigor comes years too late, especially given that Facebook's looseness with user data in 2010 led to [an FTC consent decree](#) that placed strict requirements on how it handled your information. This is a company, after all, that for years left up a detailed privacy setting that didn't do what it said. In fact, it [barely did anything at all](#).

"Facebook already had a legal obligation to not misrepresent its privacy settings and to verify the security of all third party apps on its platform and submit audits," says Sam Lester, consumer privacy fellow at the Electronic Privacy Information Center. "They utterly failed to comply with that order, which I think is clear from today's hearings."

Facebook did stop the pervasive sharing that allowed the Cambridge Analytica fiasco in 2015. And it will [introduce a redesigned settings menu](#) soon, one that at the very least puts everything in one place. The company this week proactively started pointing some users to the **Apps and Websites** setting that shows people what apps could sift through their info. All of that counts as progress. But privacy is

not a solved problem for Facebook, especially given its (repeatedly failed previous attempts) at self-correction. Zuckerberg has [spent the last 14 years](#) apologizing for privacy slip-ups. There's not much room for benefit of the doubt.

See What's Next in Tech With the Fast Forward Newsletter

A weekly dispatch from the future by Will Knight, exploring AI advances and other technology set to change our lives. Delivered every Thursday.

“For obvious reasons we're not concerned with what Facebook's fixes to this problem are,” says Lester. “They're the company that created these problems. We can't be looking to the company that caused these problems to fix them.”

If nothing else, the Cambridge Analytica has shown people what Facebook is and always has been: An alchemist that spins your data into gold. That's not going to change. But the amount of transparency Facebook gives you around it still needs to—if only Mark Zuckerberg could see it.

More Facebook

Head right [here to watch Mark Zuckerberg's testimony live on Wednesday morning at 10 am EDT](#)

Get caught up on [the rest of Mark Zuckerberg's first day of testimony](#)

Read [WIRED's previous reporting on Cambridge Analytica](#) to catch up on the fiasco that just won't quit

EXHIBIT 57

Facebook pays teens to install VPN that spies on them

Josh Constine

Exhibit
Klein v. Meta
Mario Sancho
2765

Desperate for data on its competitors, Facebook has been secretly paying people to install a “Facebook Research” VPN that lets the company suck in all of a user’s phone and web activity, similar to Facebook’s Onavo Protect app that Apple banned in June and that was removed in August. Facebook sidesteps the App Store and rewards teenagers and adults to download the Research app and give it root access to network traffic in what may be a violation of Apple policy so the social network can decrypt and analyze their phone activity, a TechCrunch investigation confirms.

Facebook admitted to TechCrunch it was running the Research program to gather data on usage habits.

Since 2016, Facebook has been paying users ages 13 to 35 up to \$20 per month plus referral fees to sell their privacy by installing the iOS or Android “Facebook Research” app. Facebook even asked users to screenshot their Amazon order history page. The program is administered through beta testing services Applause, BetaBound and uTest to cloak Facebook’s involvement, and is referred to in some documentation as “Project Atlas” — a fitting name for Facebook’s effort to map new trends and rivals around the globe.

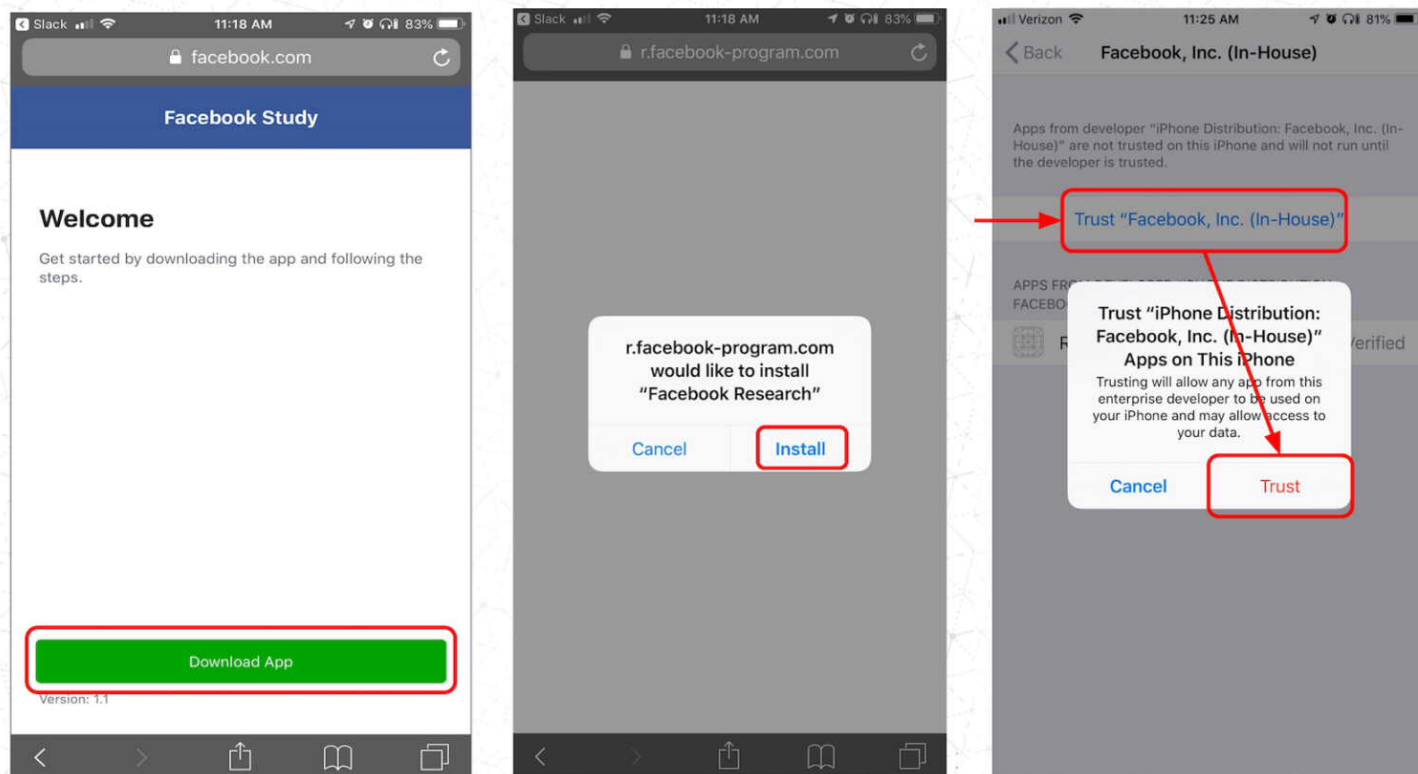
Seven hours after this story was published, Facebook told TechCrunch it would shut down the iOS version of its Research app in the wake of our report. But on Wednesday morning, an [Apple spokesperson confirmed that Facebook violated its policies, and it had blocked Facebook’s Research app](#) on Tuesday before the social network seemingly pulled it voluntarily (without mentioning it was forced to do so). You can read our full report on the development [here](#).

An Apple spokesperson provided this statement. “We designed our Enterprise Developer Program solely for the internal distribution of apps within an organization. Facebook has been using their membership to distribute a data-collecting app to consumers, which is a clear breach of their agreement with Apple. Any developer using their enterprise certificates to distribute apps to consumers will have their certificates revoked, which is what we did in this case to protect our users and their data.”

Facebook’s Research program will continue to run on Android. [Update 2/21/19: [Facebook will pull Onavo from the Google Play store and eventually shut it down](#). It will also cease to recruit users for the Android version of its Research app, though it plans other paid research initiatives.]

Facebook’s Research app requires users to ‘Trust’ it with extensive access to their data. We asked

Guardian Mobile Firewall's security expert Will Strafach to dig into the Facebook Research app, and he told us that "If Facebook makes full use of the level of access they are given by asking users to install the Certificate, they will have the ability to continuously collect the following types of data: private messages in social media apps, chats from in instant messaging apps – including photos/videos sent to others, emails, web searches, web browsing activity, and even ongoing location information by tapping into the feeds of any location tracking apps you may have installed." It's unclear exactly what data Facebook is concerned with, but it gets nearly limitless access to a user's device once they install the app.



The strategy shows how far Facebook is willing to go and how much it's willing to pay to protect its dominance — even at the risk of breaking the rules of Apple's iOS platform on which it depends. Apple may have asked Facebook to discontinue distributing its Research app.

A more stringent punishment would be to revoke Facebook's permission to offer employee-only apps. The situation could further chill relations between the tech giants. Apple's Tim Cook has repeatedly criticized Facebook's data collection practices. Facebook disobeying iOS policies to slurp up more information could become a new talking point.



Project Atlas Installation Guide

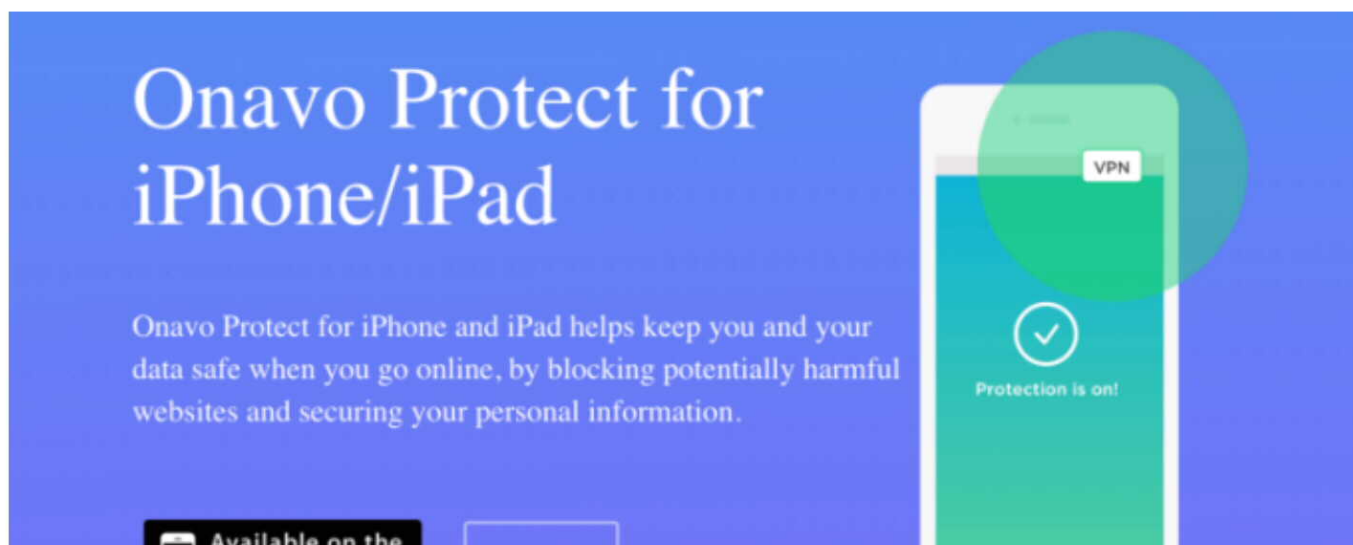
iOS

Facebook's Research program is referred to as Project Atlas on sign-up sites that don't mention Facebook's involvement

"The fairly technical sounding 'install our Root Certificate' step is appalling," Strafach tells us. "This hands Facebook continuous access to the most sensitive data about you, and most users are going to be unable to reasonably consent to this regardless of any agreement they sign, because there is no good way to articulate just how much power is handed to Facebook when you do this."

Facebook's surveillance app

Facebook first got into the data-sniffing business when it [acquired Onavo](#) for around \$120 million in 2014. The VPN app helped users track and minimize their mobile data plan usage, but also gave Facebook deep analytics about what other apps they were using. Internal documents acquired by Charlie Warzel and Ryan Mac of [BuzzFeed News](#) reveal that Facebook was able to leverage Onavo to learn that WhatsApp was sending more than twice as many messages per day as Facebook Messenger. Onavo allowed Facebook to spot WhatsApp's meteoric rise and justify paying \$19 billion to buy the chat startup in 2014. WhatsApp has since tripled its user base, demonstrating the power of Onavo's foresight.





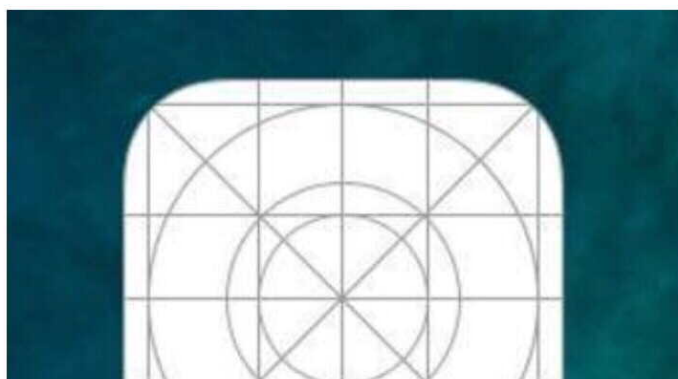
Over the years since, Onavo clued Facebook in to what apps to copy, features to build and flops to avoid. By 2018, Facebook was promoting the [Onavo app in a Protect](#) bookmark of the main Facebook app in hopes of scoring more users to snoop on. Facebook also launched the [Onavo Bolt app](#) that let you lock apps behind a passcode or fingerprint while it surveils you, but Facebook shut down the app the day it was discovered following privacy criticism. Onavo's main app remains available on Google Play and has been installed more than 10 million times.

The backlash heated up after security expert [Strafach detailed](#) in March how Onavo Protect was reporting to Facebook when a user's screen was on or off, and its Wi-Fi and cellular data usage in bytes even when the VPN was turned off. In June, Apple updated its developer policies to ban collecting data about usage of other apps or data that's not necessary for an app to function. Apple proceeded to inform Facebook in August that Onavo Protect violated those data collection policies and that the social network needed to remove it from the App Store, which it did, Deepa Seetharaman of the [WSJ](#) reported.

But that didn't stop Facebook's data collection.

Project Atlas

TechCrunch recently received a tip that despite Onavo Protect being banished by Apple, Facebook was paying users to sideload a similar VPN app under the Facebook Research moniker from outside of the App Store. We investigated, and learned Facebook was working with three app beta testing services to distribute the Facebook Research app: BetaBound, uTest and Applause. Facebook began distributing the Research VPN app in 2016. It has been referred to as Project Atlas since at least mid-2018, around when backlash to Onavo Protect magnified and Apple instituted its new rules that prohibited Onavo. Previously, a similar program was called Project Kodiak. Facebook didn't want to stop collecting data on people's phone usage and so the Research program continued, in disregard for Apple banning Onavo Protect.





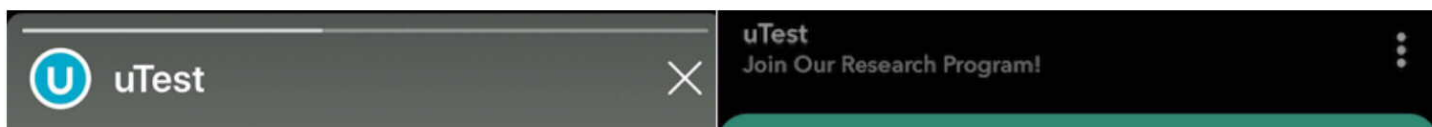
Facebook's Research App on iOS

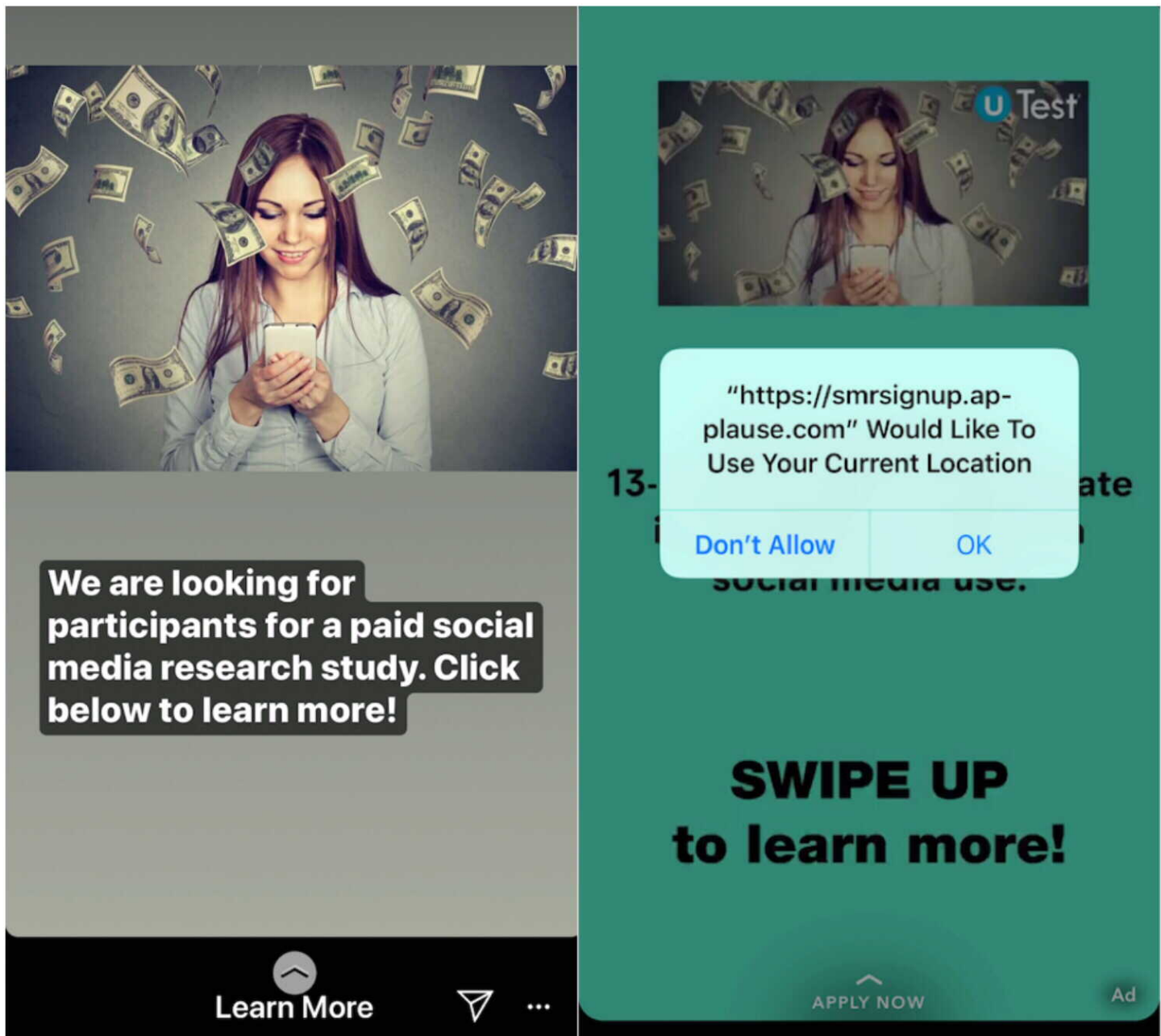
Ads (shown below) for the program run by uTest on Instagram and Snapchat sought teens 13-17 years old for a "paid social media research study." The [sign-up page](#) for the Facebook Research program administered by Applause doesn't mention Facebook, but seeks users "Age: 13-35 (parental consent required for ages 13-17)." If minors try to sign-up, they're asked to get their parents' permission with a form that reveals Facebook's involvement and says "There are no known risks associated with the project, however you acknowledge that the inherent nature of the project involves the tracking of personal information via your child's use of apps. You will be compensated by Applause for your child's participation." For kids short on cash, the payments could coerce them to sell their privacy to Facebook.

The Applause site explains what data could be collected by the Facebook Research app (emphasis mine):

*"By installing the software, you're giving our client permission to collect data from your phone that will help them understand how you browse the internet, and how you use the features in the apps you've installed . . . This means you're **letting our client collect information such as which apps are on your phone, how and when you use them**, data about your activities and content within those apps, as well as how other people interact with you or your content within those apps. You are also **letting our client collect information about your internet browsing activity** (including the websites you visit and data that is exchanged between your device and those websites) and your use of other online services. There are some instances when **our client will collect this information even where the app uses encryption**, or from within secure browser sessions."*

Meanwhile, the [BetaBound sign-up page](#) with a URL ending in "Atlas" explains that "For \$20 per month (via e-gift cards), you will install an app on your phone and let it run in the background." It also offers \$20 per friend you refer. That site also doesn't initially mention Facebook, but the instruction manual for installing Facebook Research reveals the company's involvement.





Facebook's intermediary uTest ran ads on Snapchat and Instagram, luring teens to the Research program with the promise of money

Facebook seems to have purposefully avoided TestFlight, Apple's official beta testing system, which requires apps to be reviewed by Apple and is limited to 10,000 participants. Instead, the instruction manual reveals that users download the app from r.facebook-program.com and are told to install an Enterprise Developer Certificate and VPN and "Trust" Facebook with root access to the data their phone transmits. Apple requires that developers agree to only use this certificate system for distributing internal corporate apps to their own employees. Randomly recruiting testers and paying them a monthly fee appears to violate the spirit of that rule.



```

f -[ONVEventer addDeviceDetailsToExtras:]
f -[ONVEventer events]
f -[ONVEventer setEvents:]
f -[ONVEventer setAnalyticsQueue:]
f -[ONVEventer lastFlush]
f -[ONVEventer setLastFlush:]
f -[ONVEventer sessionId]
f -[ONVEventer setSessionId:]
f -[ONVEventer seq]
f -[ONVEventer setSeq:]
f -[ONVEventer user]
f -[ONVEventer setUser:]
f -[ONVEventer setLogFileManager:]
f -[ONVEventer setAnalyticsUploader:]
f -[ONVEventer initialized]
f -[ONVEventer setInitialized:]
f -[ONVEventer applId]
f -[ONVEventer setApplId:]
f -[ONVEventer loginSecret]
f -[ONVEventer setLoginSecret:]
f -[ONVEventer eventsCounters]
f -[ONVEventer setEventsCounters:]
f -[ONVEventer .cxx_destruct]
f sub_10005F324
f sub_10005F350
f +[OnavoLogger sharedInstance]
f sub_10005F3F0
f nullsub_46
f nullsub_47
f +[OnavoLogger initDDLogger]
f -[OnavoLogger init]
f -[OnavoLogger logWithSourceFileLineNumber:]

```

Security expert Will Strafach found Facebook's Research app contains lots of code from Onavo Protect, the Facebook-owned app Apple banned last year

Once installed, users just had to keep the VPN running and sending data to Facebook to get paid. The Applause-administered program requested that users screenshot their Amazon orders page. This data could potentially help Facebook tie browsing habits and usage of other apps with purchase preferences and behavior. That information could be harnessed to pinpoint ad targeting and understand which types of users buy what.

TechCrunch commissioned Strafach to analyze the Facebook Research app and find out where it was sending data. He confirmed that data is routed to "vpn-sjc1.v.facebook-program.com" that is associated with Onavo's IP address, and that the facebook-program.com domain is registered to Facebook, according to MarkMonitor. The app can update itself without interacting with the App Store, and is linked to the email address PeopleJourney@fb.com. He also discovered that the Enterprise Certificate first acquired in 2016 indicates Facebook renewed it on June 27th, 2018 — weeks after Apple announced its new rules that prohibited the similar Onavo Protect app.

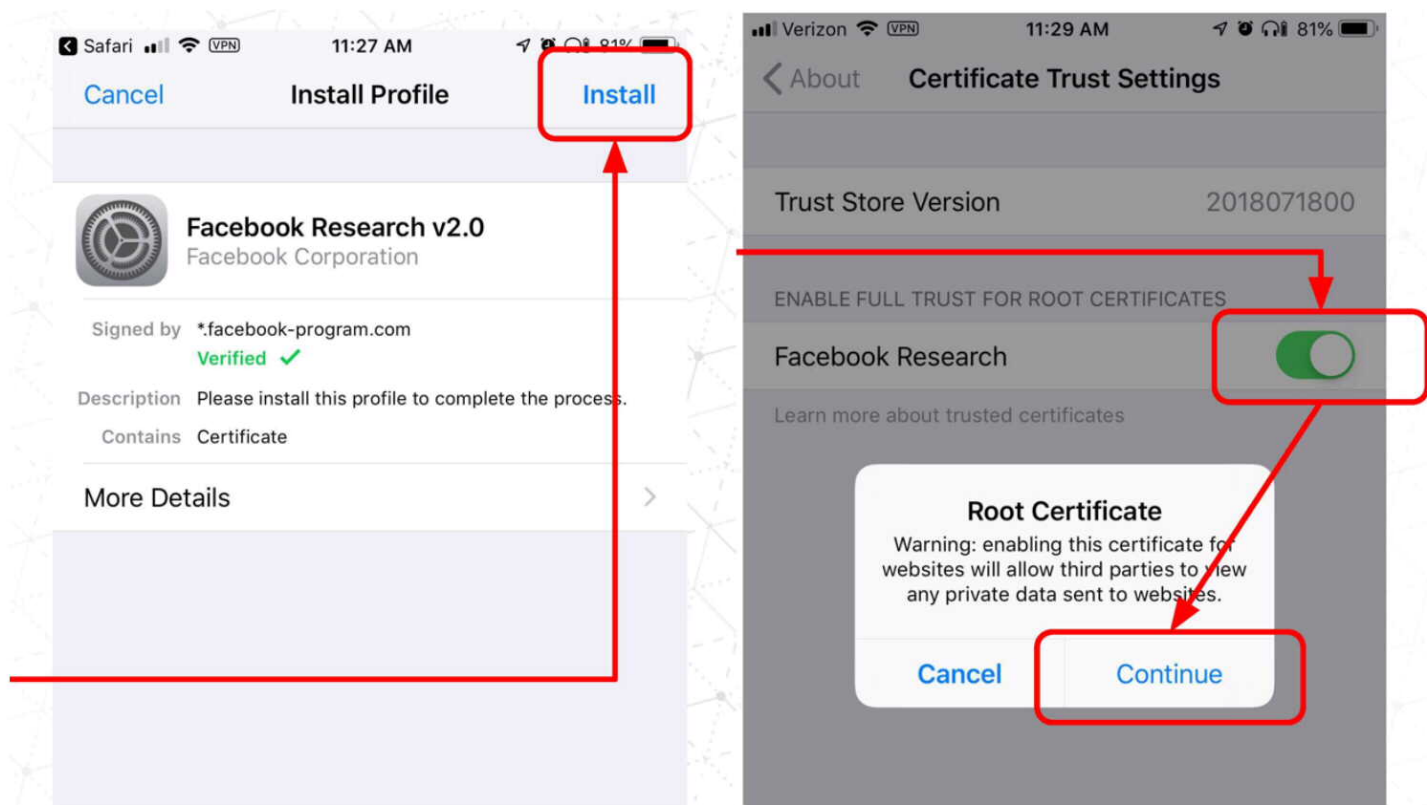
"It is tricky to know what data Facebook is actually saving (without access to their servers). The only

information that is knowable here is what access Facebook is capable of based on the code in the app. And it paints a very worrisome picture,” Strafach explains. “They might respond and claim to only actually retain/save very specific limited data, and that could be true, it really boils down to how much you trust Facebook’s word on it. The most charitable narrative of this situation would be that Facebook did not think too hard about the level of access they were granting to themselves . . . which is a startling level of carelessness in itself if that is the case.”

TechCrunch also found that [Google’s Screenwise Meter surveillance app also breaks the Enterprise Certificate policy](#), though it does a better job of revealing the company’s involvement and how it works than Facebook does.



“Flagrant defiance of Apple’s rules”

In response to TechCrunch’s inquiry, a Facebook spokesperson confirmed it’s running the program to learn how people use their phones and other services. The spokesperson told us “Like many companies, we invite people to participate in research that helps us identify things we can be doing better. Since this research is aimed at helping Facebook understand how people use their mobile devices, we’ve provided extensive information about the type of data we collect and how they can participate. We don’t share this information with others and people can stop participating at any time.”



Facebook’s Research app requires Root Certificate access, which Facebook gather almost any piece of data transmitted by your phone

Facebook's spokesperson claimed that the Facebook Research app was in line with Apple's Enterprise Certificate program, but didn't explain how in the face of evidence to the contrary. They said Facebook first launched its Research app program in 2016. They tried to liken the program to a focus group and said Nielsen and comScore run similar programs, yet neither of those ask people to install a VPN or provide root access to the network. The spokesperson confirmed the Facebook Research program does recruit teens but also other age groups from around the world. They claimed that Onavo and Facebook Research are separate programs, but admitted the same team supports both as an explanation for why their code was so similar.

Done  smrsignup.applause.com 

APPLAUSE[®]


Additional Information Needed

Thank you for your participation in the Applause Research program. We need a little bit more information. If you have the Amazon mobile app, please follow the steps below to participate.

Steps to upload a screenshot

1. Open your Amazon mobile app
2. On the Menu, tap "Your Orders"
3. Tap "Filter orders"
4. On the Time filter section, tap "Last 30 days", and then tap "Apply"
5. Take a screenshot and upload below
6. Tap Submit and you're all done!

Choose File

 1 photo

Submit

Facebook's Research program requested users screenshot their Amazon order history to provide it with purchase data

However, Facebook's claim that it doesn't violate [Apple's Enterprise Certificate policy](#) is directly contradicted by the terms of that policy. Those include that developers "Distribute Provisioning Profiles only to Your Employees and only in conjunction with Your Internal Use Applications for the purpose of developing and testing". The policy also states that "You may not use, distribute or otherwise make Your Internal Use Applications available to Your Customers" unless under direct supervision of employees or on company premises. Given Facebook's customers are using the Enterprise Certificate-powered app without supervision, it appears Facebook is in violation.

Seven hours after this report was first published, Facebook updated its position and told TechCrunch that it would shut down the iOS Research app. Facebook noted that the Research app was started in 2016 and was therefore not a replacement for Onavo Protect. However, they do share similar code and could be seen as twins running in parallel. A Facebook spokesperson also provided this additional statement:

"Key facts about this market research program are being ignored. Despite early reports, there was nothing 'secret' about this; it was literally called the Facebook Research App. It wasn't 'spying' as all of the people who signed up to participate went through a clear on-boarding process asking for their permission and were paid to participate. Finally, less than 5 percent of the people who chose to participate in this market research program were teens. All of them with signed parental consent forms."

Facebook did not publicly promote the Research VPN itself and used intermediaries that often didn't disclose Facebook's involvement until users had begun the signup process. While users were given clear instructions and warnings, the program never stresses nor mentions the full extent of the data Facebook can collect through the VPN. A small fraction of the users paid may have been teens, but we stand by the newsworthiness of its choice not to exclude minors from this data collection initiative.

Facebook disobeying Apple so directly and then pulling the app could hurt their relationship. "The code in this iOS app strongly indicates that it is simply a poorly re-branded build of the banned Onavo app, now using an Enterprise Certificate owned by Facebook in direct violation of Apple's rules, allowing Facebook to distribute this app without Apple review to as many users as they want," Strafach tells us. ONV prefixes and mentions of graph.onavo.com, "onavoApp://" and "onavoProtect://" custom URL schemes litter the app. "This is an egregious violation on many fronts, and I hope that Apple will act expeditiously in revoking the signing certificate to render the app inoperable."

Facebook is particularly interested in what teens do on their phones as the demographic has increasingly abandoned the social network in favor of Snapchat, YouTube and Facebook's acquisition Instagram. Insights into how popular with teens is Chinese video music app TikTok and meme sharing led Facebook to launch a clone called Lasso and begin developing a meme-browsing feature

called LOL, TechCrunch first reported. But Facebook's desire for data about teens riles critics at a time when the company has been battered in the press. Analysts on tomorrow's Facebook earnings call should inquire about what other ways the company has to collect competitive intelligence now that it's ceased to run the Research program on iOS.

Last year when Tim Cook was asked what he'd do in Mark Zuckerberg's position in the wake of the Cambridge Analytica scandal, [he said](#) "I wouldn't be in this situation . . . The truth is we could make a ton of money if we monetized our customer, if our customer was our product. We've elected not to do that." Zuckerberg told Ezra Klein that he felt Cook's comment was "extremely glib."

Now it's clear that even after Apple's warnings and the removal of Onavo Protect, Facebook was still aggressively collecting data on its competitors via Apple's iOS platform. "I have never seen such open and flagrant defiance of Apple's rules by an App Store developer," Strafach concluded. Now that Facebook has ceased the program on iOS and its Android future is uncertain, it may either have to invent new ways to surveil our behavior amidst a climate of privacy scrutiny, or be left in the dark.

Update 11:20pm pacific, January 29th, 2019: This article has been updated with Facebook's confirmation that it will shut down the Facebook Research app for iOS, and with our commentary on the shut down.

Update 8:01am pacific, January 30th, 2019: This article has been updated with Apple's confirmation and statement that Facebook's Research app violated its policies, and with our follow-up article on the news.

Update: 9:27am pacific, January 30th, 2019: This article has been updated to reflect that Apple forced Facebook to shut down the Facebook Research app for iOS.

Update: 11:37am pacific, January 30th, 2019: This article has been updated with a link to our follow-up report on Google shutting down its Screenwise Meter app that similarly violated Apple's policies.

Update: 7:56am pacific, February 21st, 2019: This article has been updated to reflect the news that Facebook will cease recruiting for the Android version of Facebook Research, and that it will shut down its Onavo Protect app.

Additional reporting by Zack Whittaker.